June 2018

Development of the Cybersecurity Attitudes Scale and Modeling Cybersecurity Behavior and its Antecedents

David J. Howard
University of South Florida, davidhoward@mail.usf.edu

Development of the Cybersecurity Attitudes Scale and Modeling Cybersecurity Behavior and its Antecedents

by

David J. Howard

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Arts
Department of Psychology
College of Arts and Sciences
University of South Florida

Major Professor: Michael D. Coovert, Ph.D.
Paul E. Spector, Ph.D.
Joseph A. Vandello, Ph.D.

Date of Approval:
April 30, 2018

Keywords: cyberpsychology, policy adherence, perceived vulnerability, personality, cyberclimate

Dedication

This thesis is dedicated to my husband, William Curry. Thank you for all the love and support throughout my entire academic career and especially during the time the work on this thesis was completed. I would also like to thank Roger Harville for listening to me endlessly throughout the crafting of this research. It took a long time, but I finally received a formal education. It is wonderful to know you never stopped believing that it could happen.

Acknowledgments

Thank you to Dr. Michael D. Coovert for plucking me out of obscurity and overseeing this thesis after already guiding me through the process of my undergraduate thesis. I will forever be thankful for the support, mentoring, and wisdom you provided me over the past two and a half years on this project, and the years prior. I would also like to acknowledge and thank Dr. Paul E. Spector and Dr. Joseph A. Vandello for their contributions and valuable feedback throughout the course of this thesis. Lastly, I would like to thank Dr. Stephen Stark, Dr. Michael T. Braun, and Walter C. Borman. Their assignments for classes in the first-year of the I-O program served as the backbone of this research, and their comments on those papers proved valuable as well.

Table of Contents

List of Tables

List of Figures

Abstract

As organizations have become more reliant on computers and technology to operate in a globalized world, they have also become more vulnerable to cyberattacks on their networks. The expense to organizations from cyberattacks now exceeds $400 billion USD annually. These costs highlight the need for behavioral research in the cyber domain. The first phase of this research developed an instrument to measure workers' cybersecurity attitudes. An iterative process resulted in a scale with good psychometric properties - The Cybersecurity Attitudes Scale. The scale measures two factors: cyber policy adherence attitudes and perceived vulnerability to a cyberattack. The second phase of this research used the theory of planned behavior as a theoretical framework to model the relationship between personality facets, policy adherence attitudes, perceived vulnerability, locus of control, cybersecurity climate, and cybersecurity behaviors. While the hypothesized model had poor fit for the data, there was a strong relationship between cybersecurity attitudes (i.e. policy adherence attitudes and perceived vulnerability) and dutifulness, altruism, compliance, cybersecurity climate, and cybersecurity behavior. This research provides practical value to academic researchers and organizations by providing a scale to measure cybersecurity attitudes and to help organizations better understand the nature of the antecedents that lead to cybersecurity attitudes and behavior.

Chapter One
Introduction

The emergence of new technologies, and especially information technology (IT), has had a monumental impact on how organizations conduct their business and how workers are able to perform their jobs (Valcour & Hunter, 2005). Long gone are the days of employees working with pen and paper, filing paperwork by hand, and storing massive amounts of data in a records closet. The personal computer, local-area networking, and use of the Internet has improved worker efficiency and capability, and this transition to a computerized world is still a rapidly evolving environment. In 1999, Kevin Ashton coined the term “the Internet of Things (IoT)” when describing the management of supply chains (Ashton, 2009). The term has recently gained popularity, but at the time Ashton was referring to how “things” other than just personal computers would one day be connected to the Internet. While an astute observation, it is quite possible even Ashton could not foresee the magnitude of how many devices would one day be connected to the Internet (Dorsey, Martin, Howard, & Coovert, 2017). In 2011, for the first time the number of Internet-connected devices outnumbered the population of the Earth, and that number (7 billion) is expected to more than triple by the year 2020, with analysts projecting 24 billion Internet-connected devices to be in use (Gubbi, Buyya, Marusic, & Palaniswami, 2013).

The combination of technologies such as the personal computer and the Internet with newer technologies such as smartphones, cloud computing, and virtual private networking have given rise to a workplace that reaches new heights for productivity and communication. The workplace itself has changed as it is now commonplace for many workers to have the ability to work from home or have seamless access to their company's resources whether in the office or on the road. All of this newfound access to information from anywhere in the world comes at a heavy cost: the need for organizations to protect their company's data, such as personnel information and intellectual property, through cybersecurity.

Cybersecurity belongs to a new breed of technologies referred to as "exponential technologies" (Briggs & Shingles, 2015). Until recently, the speed at which technology moved forward was defined by Moore's Law, which states that every two years technologies such as personal computing double in computing power, while the price of the technology is cut in half (Schaller, 1997). Along with technologies such as artificial intelligence, robotics, and industrial biology; cybersecurity is considered an exponential technology because its rate of advancement is moving at a much faster pace than Moore's Law describes (Briggs & Shingles, 2015; Dorsey, et al., 2017). While exponential technologies can assist organizations with faster attainment of goals and productivity, they can also have a disruptive effect on the workplace (Arena, 2014; Briggs & Shingles, 2015). Globally, the total cost to organizations from cybersecurity breaches reached over $315 billion U.S. dollars in 2014 (Grant Thornton, 2015), and this number has been increasing for the past several years. Because of the devastating financial effect cybersecurity can have on organizations and workers, the need for research on cybersecurity topics is at an all-time high.

This research aspires to add to the limited published research studying the behavioral side of cybersecurity, and the antecedents to those behaviors. For the purposes of behavioral research on the topic of cybersecurity, it is important to distinguish between information security and cybersecurity. Much like the name implies, information security refers to the protection of information and assets of an organization. Von Solms and van Niekerk (2013) present an excellent distinction between the information security and cybersecurity by stating that while cybersecurity encompasses information security (IS), it also includes the protection of the employees of the organization. The human factor in cybersecurity must be considered not only for the role humans play in protecting organization data and intellectual property, but also because humans are often the target of cyberattacks. In an effort to illustrate the human role in cybersecurity, two recent examples of cybersecurity breaches will be briefly summarized.

In late November 2014, Sony Pictures Entertainment confirmed they had been the victim of a criminal cyberattack. A purported hacktivist group (i.e. a group that hacks for ideological reasons, much like an activist) named the Guardians of Peace claimed responsibility for the attack and revealed they were stealing Sony's data for upwards of a year before their final attack. In addition to stealing up to 100 terabytes of data that included employee's salaries and social security numbers, the attackers targeted Sony's intellectual property, including four feature films that were uploaded to the Internet prior to release (Zetter, 2014). Additionally, using the commercially available wiping program Rawdisk, the attackers were able to completely wipe and destroy the information on Sony's corporate computers.

In June 2015, the Office of Personnel Management (OPM) announced its computer network had been breached and that 4 million employees' records had been stolen (Barrett, Yadron, & Paletta, 2015). On July 9, 2015, the news got even worse as OPM confirmed its initial estimate was far below the actual figure, and that the records of 21.5 million Americans who had undergone background security checks had their personal information stolen (Zengerle & Cassella, 2015). Later it was discovered the information stolen included the fingerprints of 5.6 million federal employees, many with top-secret security clearances (Greenberg, 2015).

In both of these cyberattacks, the access to the organizations' networks was obtained through a social engineering technique known as spear-phishing (Bort, 2014; Kelly, 2015), a tactic where an employee is targeted by an attacker and then the attacker sends a fraudulent email to the user in hopes the employee clicks on a URL link or an attachment in the email that deploys malware (e.g. viruses, Trojan horse, keyloggers) on their computer (Dorsey et al., 2017). Almost one million new instances of malware were created each day last year (Symantec, 2015). Spear-phishing is an increasingly popular social engineering technique to distribute malware that is designed to prey upon the naivety and inexperience of workers. Large organizations, such as the two aforementioned examples, are not the only companies being attacked either. In 2014, 60 percent of all targeted attacks were directed at small and medium sized organizations (i.e. companies with fewer than 2,500 employees; Symantec, 2015); illustrating the need for cybersecurity research that benefits all organizations and employees.

Social Engineering

Social engineering is the centerpiece of the human component of cybersecurity and is defined as gaining unauthorized access to computer networks through the use of psychological tricks, deception, or manipulation (Erbschloe, 2005; Abraham & Chengalur-Smith, 2010; Dorsey et al., 2017). The employees of organizations are the targets of social engineering tactics because they are the most vulnerable part of the cybersecurity environment and are much easier and less time-consuming for hackers to attack than trying to gain intrusion through a breach prevention plan that an organization has in place (Krombholz, Hovel, Huber, & Weippl, 2014).

Krombholz et al. (2014) details four approaches of social engineering attacks: physical, social, technical, and socio-technical. A physical approach to social engineering would occur if the attackers had physical access to an organization's information; whether that entailed going through the trash of the organization or simply looking for post-it notes containing passwords on an employee’s desk. When using the social approach, the attacker relies on persuading the victim through developing a relationship with them or by portraying an authority figure to the victim. An example of using the social approach would be for an attacker to call an employee at an organization’s help desk and state that they are a traveling manager and need access to the company’s network, thus manipulating a password from the employee through a telephone conversation (Krombholz et al., 2014).

An example of the technical approach to social engineering would be to use open source information that is readily available on the Internet (e.g. information that is available on a person’s social media profile) and use that information to manipulate an employee into giving a password or other access to the network. Lastly, the socio-technical approach is a combination of the social and technical approach. In addition to spear-phishing, another example of the socio-technical approach is baiting. Baiting occurs when an attacker leaves media containing malware, such as a USB flash drive, near or in an office building with the intention that the person who finds the media will place it in an office computer (Krombholz et al., 2014; Dorsey et al., 2017). Once the USB drive is placed in a computer, the malware can deploy itself undetected and spread throughout the organization’s network.

The rise in the number of malware created each year, the total costs to organizations of cybersecurity breaches, and the increasingly manipulative social engineering techniques used by attackers prove a need for behavioral research in this domain. If organizations can ascertain which factors may make employees more susceptible to social engineering techniques, they could administer an assessment to assist with screening out potentially harmful employees prior to offering employment. Furthermore, the assessment could be administered to current employees to help identify which employees might be most in need of comprehensive cybersecurity training. Although there has been a lack of behavioral research regarding cybersecurity in general, recent work has begun in the information security behaviors domain (Siponen, 2000; Herath & Rao, 2009; Guo, Yuan, Archer, & Connelly, 2011; Guo 2013). This study aims to better understand the relationship between personality facets as an antecedent of cybersecurity behaviors within a framework based on the theory of planned behavior.

Personality

This research seeks to extend current personality and Industrial / Organizational psychology (I-O) research to the cybersecurity domain. Psychology researchers have been interested in personality for over 100 years, as the first appearance of personality as a topic of study in an academic journal occurred in 1906 in the *Journal of Abnormal Psychology* (Barenbaum & Winter, 2008). Throughout the history of personality research, one topic has remained much studied, while also remaining much debated: the analysis of the factor structure of personality traits. Early research in determining personality structure focused on using a lexical approach to identify personality traits by studying trait-descriptive words (Goldberg, 1993).

Raymond Cattell, one of the early pioneers of personality structure research, built upon the lexical approach by using factor analysis to study the 4,504 trait-descriptive terms that Gordon Allport and Henry Odbert compiled in 1936 (Goldberg, 1993; Cattell, 1943; Allport & Odbert, 1936). Cattell first categorized the massive list of words into 171 variables, and then further reduced the number to 60 provisional personality titles. These titles included categories such as “infantile / hostile” and “facile / forward / verbose” (Cattell, 1943). Using factor analytic techniques, Cattell later settled on 12 primary factors of personality (Barenbaum & Winter, 2008): Warmth (A), Reasoning (B), Emotional Stability (C), Dominance (E), Liveliness (F), Rule-Consciousness (G), Social Boldness (H), Sensitivity (I), Vigilance (L), Abstractedness (M), Privateness (N), Apprehension (O). Ultimately, his work led him to create the 16PF personality questionnaire, which added four more factors: Openness to Change (Q1), Self-Reliance (Q2), Perfectionism (Q3), Tension (Q4) (Russell, Cattell, Cattell, Cattell, & Karol, 1994).

The Big Five

Several other researchers attempted to replicate Cattell's 16-factor solution, but were unsuccessful, and in each case a 5-factor solution was found (Fiske, 1959; Tupes & Christal, 1961, Barrick & Mount, 1991). As years passed, other alternatives to Cattell's 16-factor solution to personality structure gained popularity, such as Eysenck's (1991) 3-factor P-E-N model (Psychoticism, Extraversion, Neuroticism) and Jackson's 6-factor PRF solution (Barenbaum & Winter, 1998). However, there was not a lot of consensus among researchers regarding personality factor structure until the 1990s, when the "Big Five" emerged as the dominant taxonomy. Although there has been some disagreement on the names of the Big Five factors (Goldberg, 1993), many researchers today have settled on these five: Extraversion, Agreeableness, Conscientiousness, Emotional Stability, and Openness-to-Experience (John, Naumann, & Soto, 2008).

Extraversion is the personality factor associated with sociability and individuals high in this personality trait are talkative, active, and express positive emotion (Barrick & Mount, 1991; John, Naumann, & Soto, 2008). Emotional Stability is sometimes referred to in a negative manner as Neuroticism, though there is some argument these constructs are at opposite ends of a spectrum. Individuals high in Emotional Stability would be calm and even-tempered, whereas an individual high in Neuroticism would be anxious or easily angered. Agreeableness is the factor associated with an individual's interpersonal skills and includes traits such as altruism, friendliness, and tolerance (Barrick & Mount, 1991; John, Naumann, & Soto, 2008). Individuals high in Conscientiousness are responsible, organized, and hardworking. Lastly, Openness-to-Experience (also known as Intellectence) is the factor associated with an individual's willingness to experience new things, and those high in Openness-to-Experience exhibit traits such as being imaginative, original, and adventure-seeking (Barrick & Mount, 1991; John, Naumann, & Soto, 2008).

To illustrate the dominance of the Big Five taxonomy in recent years, John, Naumann, and Soto (2008) presented a histogram depicting the number of publications related to the Big Five taxonomy versus the combined total of Cattell's 16PF and Eysenck and Eysenck's P-E-N model in 5-year intervals starting in 1980 to the present. The Big Five taxonomy was essentially nonexistent in 1980, but in 2006 the taxonomy was represented in over 300 articles annually; a stark contrast to the fewer than 50 combined using the Cattell or Eysenck and Eysenck approach. The emergence of the Big Five's dominance in Industrial / Organizational psychology research can be partly explained by Goldberg's (1993) suggestion that the Big Five taxonomy could prove a useful framework to study "personality-oriented job analyses, reliable measures of job-related personality traits, and the optimal procedures for linking applicants' personality with job requirements" (p. 32).

Barrick and Mount (1991) agree with Goldberg's position, and further posit that the Big Five framework provides a meaningful taxonomy to formulate and test hypotheses regarding non-cognitive individual differences. Their seminal meta-analysis examined the relationship between personality factors and ratings of three job performance criteria (training proficiency, job proficiency, and personnel data), and found that Conscientiousness was a predictor of ratings of job performance across jobs included in their meta-analysis. Additionally, they found Extraversion predicted job performance in sales and managerial jobs, and that Extraversion and Openness-to-Experience predicted training proficiency outcomes (Barrick & Mount, 1991). Though job performance is one of the main criteria of I/O psychology research (some say “the criterion”), personality factors are valid predictors of other work outcomes too, such as Neuroticism predicting job satisfaction, burnout, and turnover (Thoreson, Kaplan, Barsky, Warren, & de Chermont, 2003).

Facet-Level Approaches

Another approach to analyzing personality factors is to examine personality traits at the facet level. Costa and McCrae developed the Revised NEO Personality Inventory (NEO-PI-R; Costa & McCrae, 1992) to assess 30 personality traits, with each of the Big Five personality factors containing six facet-level traits. As an example to elucidate the facet-level structure of the NEO-PI-R, in Costa and McCrae’s taxonomy Agreeableness is a factor consisting of the following six traits: Trust, Straightforwardness, Altruism, Compliance, Modesty, and Tender-Mindedness. The other 24 traits are split evenly among the other four Big Five personality factors. Costa and McCrae (1992a) found good discriminant validity for the 30-trait structure after controlling for the Big Five factors. DeYoung, Peterson, and Quilty (2007) introduced another alternative to the Big Five that uses a facet-level taxonomy, a 10-trait facet-level approach with each Big Five factor housing two facets. In contrast to the Costa and McCrae taxonomy, in the DeYoung et al. (2007) taxonomy, Agreeableness is split into the two facets: Compassion and Politeness.

Recently, debate has occurred on whether a broad or narrow approach was preferable in personality research (Judge, Rodell, Klinger, Simon, & Crawford, 2013). When considering which approach to employ in research, the Judge et al. (2013) meta-analysis highlighted the need for researchers to consider the concept of construct correspondence. Construct correspondence refers to the relationship between the specificity of predictors and criteria. Fishbein and Ajzen first expounded on construct correspondence in their research on attitudes predicting behavior (Judge, et al., 2013). Fishbein and Ajzen authored the Theory of Reasoned Action, which states that attitudes and social norms predict intentions, with intentions subsequently predicting behavior. They argue that to maximize prediction, “attitudes must be conceptualized and measured at the same level of specificity as the behaviors they seek to predict” (Judge et al., 2013, p. 879). While the concept of construct correspondence was originally applied in attitude-behavior relations, it has also been applied in trait-behavior relations (Judge, et al., 2013). Judge et al. (2013) found mixed support for construct correspondence in their meta-analysis on the relationship between personality traits and job performance. However, one of their findings that supports the notion of construct correspondence was that the DeYoung, et al. (2007) facets explained more variance in task and contextual performance than in overall job performance.

Personality and Cybersecurity

Although there has been a recent upswing in research related to the cybersecurity behaviors of employees (Hu, Dinev, Hart, & Cooke, 2012; Guo, 2013), there has been minimal research conducted examining the relationship between personality factors and cybersecurity behaviors. There are two known studies examining the relationship between personality and cybersecurity behaviors that are currently unpublished (Dreibelbis, 2016; Martin, 2017). Dreibelbis (2016) found that Conscientiousness, Agreeableness, and Openness-to-Experience were significantly related to cybersecurity behaviors, while Martin (2017) was unable to replicate the conscientiousness to cyber-related behavior relationship at the personality factor-level. The research I am proposing seeks to add to the scientific contribution of the Dreibelbis (2016) and Martin (2017) studies by examining how personality *facets* predict cybersecurity attitudes, rather than solely examining the relationships at the factor-level.

Modeling Personality Facets, Cybersecurity Attitudes, and Behavior

One of the goals of this research is test a model of the relationship between personality facets, cybersecurity attitudes, cybersecurity climate, perceived behavioral control, and cybersecurity behaviors. When considering whether to measure Big Five personality factors or facet-level traits for this study, there are two factors supporting the measurement of personality at the facet-level. First, personality will be predicting cybersecurity attitudes, which is a very specific type of attitude. Thus, taking construct correspondence into account, a narrower measure of personality might best predict a narrow attitude. Second, when examining the definitions for the Big Five personality factors versus the NEO-PI-R facets, the NEO-PI-R facets make more theoretical sense to use as predictors of cybersecurity attitudes. For example, one might have difficulty drawing a theoretical connection between Extraversion and cybersecurity attitudes; however, it is logical that someone who is high in the trait Positive Emotions would be "higher" in cybersecurity attitudes than someone who is low on the trait.

For this research, I will test a model that refines the Theory of Planned Behavior into a cybersecurity context, with locus of control, cybersecurity attitudes, and cybersecurity climate predicting cybersecurity behaviors. The model will be further modified to examine how personality facets predict cybersecurity attitudes.

Theoretical Framework

When researching how personality facets predict employees' cybersecurity attitudes (and attitudes in general), it is important to have a sound theoretical base. Ajzen's theory of planned behavior expands upon the theory of reasoned action by concluding that intentions to commit behaviors can be predicted with greater accuracy by three constructs: subjective or social norms, attitudes toward the behavior, and perceived behavioral control (Ajzen, 1991). When applying the theory, Ajzen stresses the importance of measuring *perceived* behavioral control and not actual behavioral control. According to Ajzen's theory, perceived behavioral control, along with intention, predicts future behavior. Additionally, social norms and attitudes lead to behavioral intention. Social norms refer to the perceived social pressure to perform a coinciding behavior, and attitude refers to the degree that a person views a behavior as favorable or unfavorable (Ajzen, 1991). Figure 1 represents the constructs from Ajzen's journal article *The Theory of Planned Behavior* (1991).

Support for use of the theory of planned behavior for cybersecurity research can be garnered from previous research comparing the use of the technology acceptance model versus the theory of planned behavior when predicting intentions in the information security realm (Mathieson, 1991). Furthermore, Siponen (2000) supports the use of the theory of planned behavior in his conceptual paper on computer security. Moreover, empirical studies have used the theory of planned behavior to study the Internet behavior of individuals in a home setting (Anderson, 2005; via Herath & Rao, 2009) and to study Internet behavior and cultural differences between Americans and South Koreans (Dinev, Goo, Hu, & Nam, 2006). Additionally, Beck and Ajzen (1991) used the theory of planned behavior to predict dishonest behaviors such as theft and lying; behaviors that would be considered counterproductive work behaviors if they occurred in the workplace. In an attempt to provide a more accurate fit of our variables of interest, the model Ajzen proposed will be adapted to a cybersecurity context for the purposes of this research. The construct "attitudes" will be adapted to "cybersecurity attitudes", the construct “social norms” will be adapted to “cybersecurity climate” and “behavior” will be changed to “cybersecurity behaviors”. Figure 2 displays a model of the theory of planned behavior with the adapted constructs.

Personality Facets Relating to Cybersecurity Attitudes

With the conceptual adaptation of the theory of planned behavior complete, focus is brought to the personality facets hypothesized to relate to cybersecurity attitudes. One of the personality factors that has been previously hypothesized to relate to cybersecurity behaviors is conscientiousness (Dreibelbis, 2016; Martin, 2017). As mentioned above, both the Dreibelbis (2016) and Martin (2017) studies examined conscientiousness at the factor-level and found mixed results regarding conscientiousness being able to predict cybersecurity behaviors. Therefore, this research will focus on examining the facets of conscientiousness believed to be most predictive of attitudes (and subsequently behavior). The facets of Conscientiousness include Order, Dutifulness, Competence, Achievement-Striving, Self-Discipline, and Deliberation (Costa & McCrae, 1992; via Judge et al., 2003). Descriptions of Order refers to those who are well-organized and methodical. Individuals high in the trait Dutifulness are ethical and governed by conscience. Descriptions of Self-Discipline include the ability to carry out tasks and being self-motivated. Individuals high in Deliberation think carefully before acting and are cautious (Judge et al., 2013). Theoretically, these four facets of Conscientiousness should best be able to predict to cybersecurity attitudes, and thus are hypothesized to be positively related to cybersecurity attitudes.

Hypothesis 1A: Order will be positively related to cybersecurity attitudes.

Hypothesis 1B: Dutifulness will be positively related to cybersecurity attitudes.

Hypothesis 1C: Self-Discipline will be positively related to cybersecurity attitudes.

Hypothesis 1D: Deliberation will be positively related to cybersecurity attitudes.

The facets of Agreeableness include Altruism and Compliance (Costa & McCrae, 1992). Descriptions of Altruism include being helpful, generous, and having an active concern for others (Judge et al., 2013). Compliance can be defined as conforming to official instructions. Individuals high in Altruism and Compliance would likely to be receptive to following cybersecurity policies in the workplace and be more likely to adhere to policy.

Hypothesis 2A: Altruism will be positively related to cybersecurity attitudes.

Hypothesis 2B: Compliance will be positively related to cybersecurity attitudes.

The facets of Openness-to-Experience include Fantasy and Ideas (Costa & McCrae, 1992). The trait Fantasy describes those who are lost in thought and prone to daydreaming. (Judge et al., 2013). Individuals high in Fantasy might eschew an organization's policies and have a negative attitude toward rules and policies. The trait Ideas describes someone with intellectual curiosity and willingness to try new ideas. An individual high in Ideas might be enthusiastic about learning cybersecurity policies and ways to combat possible cyberattacks.

Hypothesis 3A: Fantasy will be negatively related to cybersecurity attitudes.

Hypothesis 3B: Ideas will be positively related to cybersecurity attitudes.

Positive Emotions is a facet of Extraversion, and those high in Positive Emotions exhibit are high-spirited and optimistic (Judge et al., 2013). Individuals high in Positive Emotions would likely have a positive attitude with regards to cybersecurity practices and have a positive attitude in general.

Hypothesis 4: Positive Emotions will be positively related to cybersecurity attitudes.

In addition to the relationships between personality facets and cybersecurity attitudes, the following hypothesis represents the subsequent path from cybersecurity attitudes to cybersecurity behavior in Ajzen's (1991) theoretical framework for the relationship between locus of control, social norms, attitudes, intentions, and behavior.

Hypothesis 5: Cybersecurity attitudes will be positively related to cybersecurity behaviors.

Organizational Climate

Another variable that likely affects whether an employee commits good cybersecurity behaviors is the worker's organizational climate. Ehrhart, Schneider, and Macey (2014) formally define organizational climate as "the shared meaning organizational members attach to the events, policies, practices, and procedures they experience and the behaviors they see being rewarded, supported, and expected". Organizational climate, and climate research in general, evolved from the Lewin's Gestalt psychology experiments in the 1930s and qualitative observations of organizational behavior in the 1960s conducted by Likert (1961) and Barker (1965) (see also Denison, 1996). These early qualitative observations included administration of survey instruments to employees to assess behavioral and social aspects of the workplace (Schneider & Barbera, 2014).

One of the aspects of organizational climate that differentiates the construct from organizational culture is the focus on quantitative analysis. Litwin and Stringer (1968) constructed the first widely used instrument to measure organizational climate and the measure focused on six facets of climate: risk, rewards, structure, support, tolerance, and individual responsibility (Schneider & Barbara, 2014). The trend of using quantitative data from surveys to measure climate continues to this day. However, unlike personality research, where a taxonomy like the Big Five has become the dominant structure, organizational climate researchers still debate the number of dimensions to measure, as evidenced by Patterson et al.'s (2005) recent work identifying a 17-factor solution. While no consensus on the dimensionality of climate has yet been reached, one thing is consistent among researchers regarding the structure of organizational climate: the construct is multi-dimensional.

Throughout its history, there have been three main areas of criticism with regard to organizational climate research (Ehrhart, Schneider, and Macey, 2014). The first area of criticism concerns the levels of analysis in climate research. Psychological climate can be defined as "the individual differences in perceptions of work environments and the significance of these perceptions" (Burke, Borucki, & Kaufman, 2002; Schneider & Barbera, 2014, p. 108). While organizational climate is conceptualized as a unit, group, or organizational-level construct, psychological climate operates at the individual level. Often times researchers administering surveys purporting to measure organizational climate include measures of both organizational climate and psychological climate on the same instrument. This research will focus on cybersecurity climate as a psychological climate variable, as we will be measuring individuals that do not belong to the same organization or team.

A second initial area of criticism regarding climate research that has since subsided is the overlap between organizational climate and criterion such as job satisfaction (Ehrhart, Schneider, & Macey, 2014). However, prior research (Schneider & Snyder, 1975) was able to empirically separate the constructs with the result being climate refers to the work environment, and affect is associated with attitudes. This separation lends support to using the theory of planned behavior to study organizational outcomes as there is empirical support providing a clear distinction between the two constructs, at least when they are measured properly.

The third area of criticism originated from the lack of consistent findings when organizational climate was used as a variable to predict outcomes such as job performance

(Hellreigel & Slocum, 1974; Ehrhart, Schneider, & Macey, 2014). While Schneider (1975) responded to the initial critique by stating that organizational climate scales were very broad measures and could not be expected to adequately predict specific outcomes (Ehrhart, Schneider, & Macey, 2014), one could argue that job performance is a broad criterion and there is a conceptual match as far as the level of specificity of the two constructs is concerned. However, one lasting impact from Schneider's (1975) article was his call for climate research to study specific climates, also known as focused climates. While Schneider perhaps is credited as the forefather of focused climate, he argues in his article that researchers had long been studying specific climates (e.g. his example of Fleishman's work in 1953 that was essentially an examination of a climate for leadership).

Focused Climates (Strategic and Process)

Schneider's approach is essentially a consideration of the aforementioned concept of construct correspondence. Again, Fishbein and Ajzen's work was focused primarily on the relationship between attitudes and behavior, and they opined that behaviors are best predicted when they are conceptualized and measured at the same level of specificity as attitudes. Matching specificity of constructs using construct correspondence to match predictors with criterion has occurred in other domains, including personality (Hough & Furnham, 2003; Judge, Rodell, Klinger, Simon, & Crawford, 2013) and this study seeks to examine the concept of construct correspondence in an organizational climate context as well.

In defining focused climates, Schneider, Ehrhart, and Macey (2011) offer further categorization: strategic and process climates. The difference between strategic and process climates lies in what each is trying to address. Strategic climates are concerned with specifically addressing outcomes that organizations seek to achieve (Ehrhart & Raver, 2014). Examples of strategic climates include the two most-studied focused climates: safety climate and service climate. Process climates refer to those climates that are focused on internal processes that help support the desired outcomes. An example of a process climate would be the diversity climate of an organization (Ehrhart & Raver, 2014).

The majority of climate research today occurs in the various strategic climate domains (Ehrhart, Schneider, & Macey, 2014). The proposed construct of this research, cybersecurity climate, would be considered a strategic climate much in the same vein as safety climate. Safety climate is defined as “the shared employee perceptions about the relative importance of safe conduct in their occupational behavior” (Zohar, 1980). Safety climate has been found to be a significant predictor of specific-level outcomes such as safety knowledge, safety participation, and safety compliance (Griffin & Neal, 2000) and other focused climates such as service climate also have empirical support (Johnson, 1996) in the climate literature. Thus, this study seeks to establish a similar relationship between cybersecurity climate and cyber-related outcomes.

Cybersecurity Climate

This research will use the operationalization of cybersecurity climate that Kessler, Pindek, Kleinman, Andel, and Spector (2016) propose: “a multidimensional construct that consists of policies, practices, and procedures aimed at promoting the secure handling of confidential data (p. 9).” This definition is similarly structured to the definitions of organizational climate and safety climate, and the Kessler et al. (2016) research is itself an application of safety climate research to a cybersecurity context. One consideration when measuring a construct so similarly to another is that the instruments used to measure each similar construct may lack discriminant validity. This might be a problem that exists in climate research in general, but specifically in strategic climates when it is possible that multiple closely defined strategic climates are being measured simultaneously and discriminant validity is not confirmed as part of primary studies. Recent research found that multiple strategic climates (i.e. safety climate, violence prevention climate, and civility climate) were similarly predictive of organizational outcomes (workplace hazards; Gazica & Spector, 2016). A secondary focus of this research will explore this potential issue by administering a cybersecurity climate scale along with a safety climate measure to examine whether the two climate constructs are different from one another.

Research Question 1: Will a measure cybersecurity display discriminant validity from a measure of safety climate (i.e. exhibit a correlation between the two measures that does not suggest multicollinearity)?

This research question is particularly relevant for this research as the one published instrument that measures a similar construct to cybersecurity climate was adapted directly from safety climate scales (Chan, Woon, & Kankanhalli, 2005). Chan et al. created a 27-item information security climate scale based on eight safety climate scales and their scale exhibited good psychometric properties, but the authors did not check to see whether the instrument displayed discriminant validity from the safety climate scales on which it was based. While my research question proposes to examine the relationship between safety climate and cybersecurity climate, my hypothesis regarding cybersecurity climate seeks to measure it as a predictor for cybersecurity behavior, similar to Neal and Griffin's (2004) findings that safety climate predicted safety behavior.

Hypothesis 6: Cybersecurity climate will be positively related to cybersecurity behavior.

Locus of Control

In addition to the hypothesized relationships between facets of personality, cybersecurity attitudes, cybersecurity climate, and behaviors; the remaining antecedent of behavior represented in the theory of planned behavior is the relationship between locus of control and behavior. Locus of control is a personality variable that explains why some people attribute control of events to themselves or to outside forces (Spector, 1988). Those who attribute control of events to themselves are higher on internal locus of control, and those who attribute control of events to others or the environment are high on external locus of control. Prior research has focused on locus of control and its association with several organizational variables, including motivation, performance, and compliance with authority (Spector, 1982). Particularly relevant to this study, Coovert and Goldstein (1980) found internal locus of control to be positively related to attitudes about computer use and Hawk (1989) found those who were high in external locus of control held less positive attitudes toward computer-based information systems when user involvement was considered.

Hypothesis 7: Locus of control will be positively related to cybersecurity behaviors.

Chapter Two
Pilot Study – Development of the Cybersecurity Attitudes Scale
Method

The first hurdle to modeling how personality, perceived behavioral control, cybersecurity attitudes, security climate, and behavior fit together in a cybersecurity context is that there is no instrument to measure cybersecurity attitudes. The lack of such an instrument is the impetus for the first part of this research – to develop a scale to measure cybersecurity attitudes. I created the Cybersecurity Attitudes Scale (CAS) as an 8-item scale informed by literature review, an unnamed scale created by Workman, Bommer, and Straub (2009), and one item adapted from Herath and Rao's (2009) Policy Compliance Intentions scale. The items were constructed using single-statement item structure and a five-point Likert scale for response. A sample item from the CAS is: "I feel it is necessary to use strong passwords for my applications at work." This version of the instrument is displayed in Appendix A.

To refine the CAS instrument before administration to a sample with all the other study's measures, a pilot study was conducted to analyze the underlying factor structure of the scale. A subject matter expert was asked to review the items of the scale for redundancy and face validity. Unable to locate the exact number of participants necessary to determine reliability of an 8-item instrument, the scale construction parameters detailed in Spector's *Summated Rating Scale Construction* (1992) were used. Spector (1992) states that a sample of 100 – 200 is adequate for assessing reliability of a scale. An additional rule of thumb for the number of participants needed to conduct an exploratory factor analysis on a scale is 10 participants for every item. Using the rule of thumb for this pilot study, a total of 80 participants would be necessary. To err on the side of caution, the pilot study was submitted to the University of South Florida (ID: Pro 00028710) with a minimum of 100 participants necessary.

Since the instrument measures attitudes about cybersecurity in the workplace, participants were limited to University of South Florida psychology students who are currently employed and state they are aware that their organization has information security / cybersecurity policies in place. The participants were also asked to provide their gender and age. The survey was administered anonymously through Qualtrics and participants were able complete the scale in approximately 5 minutes. The participants were paid 0.5 SONA points compensation for completion of the pilot study.

Results

In March 2017, the collection of data for the pilot study was stopped by removing the ability for potential participants to sign up for the study in SONA. A dataset with 167 participants was then exported. An exploratory factor analysis (EFA) was conducted on the data using SPSS 24. Principal axis factoring was used as the extraction method for the EFA. The original analysis did not have a clear indication of how many factors were present in the data. There were three eigenvalues over 1 (2.06, 1.54, and 1.20), and while the scree plot did not have much of an "elbow", what bend there was occurred at the third eigenvalue. Further analysis was conducted by using both direct oblimin and varimax rotation to extract a three-factor solution. There was little difference between the solutions. Four of the items were cross-loading on multiple factors in this solution. A two-factor solution was then extracted by using direct oblimin and varimax rotation. Again, there was little difference between the results of the two rotation methods. This analysis showed six items to load well on only one factor, with two of the items, "I believe it is more important to get my work done in a timely fashion than to follow cybersecurity policies” (-.030 on factor 1 and .034 on factor 2) and “I feel it is inconvenient to have different passwords at work for different applications” (.034 on factor 1 and .019 on factor 2), not loading on either factor. The remaining items that loaded on their respective factors were examined, and conceptually the factors appeared to be “cyber policy adherence attitudes” and “perceived vulnerability attitudes”. The EFA pattern matrix is presented in table 1.

Table 1
Pattern Matrix of the Exploratory Factor Analysis of the CAS

	Factor	
	1	2
Item 1	.67	.12
Item 2	.94	.11
Item 3	-.03	.03
Item 4	.52	-.13
Item 5	-.13	.88
Item 6	.03	.02
Item 7	.15	.62
Item 8	-.02	.48

Study 1 Administration of the 8-item version of the CAS

Chapter Three
Study 1 – Administration of the 6-Item CAS
Method

Once the EFA was conducted on the initial sample, I restarted the collection of data using the new 6-item version of the scale that eliminated the two items that did not load on either factor (Appendix B). Data collection resumed in March 2017 and the survey was available to University of South Florida SONA participants through the remainder of the Spring 2017 semester (May 2017). A total of 452 students participated from March 2017 to May 2017. The participants had a mean age of 21.84 years ($SD = 3.53$). There was a more even split for gender than usual for SONA participants, with 66% ($n = 300$) of the sample female, and 34% ($n = 152$) male.

Results

A confirmatory factor analysis was conducted on the data from the 452 participants using MPlus 7.3 (Muthén & Muthén, 1998-2012). The first model tested was a correlated two-factor structure reflected by the results of the pilot study EFA (i.e. cyber policy adherence attitudes correlated with perceived vulnerability attitudes). The model fit indices for this model are as follows: $\chi^2 = 39.15$, $df = 8$, $p < 0.01$, RMSEA = 0.09 [0.07, 0.12], CFI = 0.92, TLI = 0.84, SRMR = 0.06. The one-factor model (i.e. overall cybersecurity attitudes) was examined next and had the following fit indices: $\chi^2 = 105.86$, $df = 9$, $p < 0.01$, RMSEA = 0.15 [0.13, 0.18], CFI = 0.74, TLI = 0.57, SRMR = 0.09. These results indicate that the one-factor model fit the data much worse than the correlated two-factor model. However, some of the fit indices of the two-factor model were still less than commonly accepted rules of thumb. In particular, the TLI = 0.84

was a bit low and the RMSEA = 0.09 was a bit high. Therefore, I wrote two additional items for each factor that attempted to measure policy adherence and perceived vulnerability instead of a general cybersecurity attitude.

Chapter Four

Study 2 – Administration of the 10-item version of the CAS

Method

This new 10-item version of the scale was ready to administer to a new sample. The two new “cyber policy adherence” items are “I feel it is in my best interest to follow my organization’s cybersecurity policies” and “I feel it is in my employer’s best interest to hire individuals who follow the organization’s cybersecurity policies”. The two “perceived vulnerability” items are “I feel it is possible that an employee browsing the Internet could lead to a cyberattack at my organization” and “I feel I am vulnerable to my personal information being stolen from my organization in a cyberattack”.

Participants

Data collection to conduct a confirmatory factor analysis on the new 10-item version of the CAS began in the fall 2017 semester. The survey was available to SONA participants through November 2017. After removal of responses from participants who did not complete the instrument, 287 students participated in this portion of the study. The participants were 74.6% ($n = 214$) female and 25.1% ($n = 72$) male, with one respondent not answering the question ($n = 1$, 0.3%). The average age of the participants was 21.09 years ($SD = 3.97$).

Results

I conducted a correlated two-factor model confirmatory factor analysis on this data and found the following model fit indices: $\chi^2 = 75.90$, $df = 34$, $p < 0.01$, RMSEA = 0.07 [0.05, 0.09], CFI = 0.98, TLI = 0.97, SRMR = 0.05. I then conducted a single-factor confirmatory factor-analysis on this data as well, and the model fit indices were as follows: $\chi^2 = 846.87$, $df = 35$, $p <$

0.01, RMSEA = 0.28 [0.27, 0.30], CFI = 0.52, TLI = 0.39, SRMR = 0.23. The correlated two-factor model fit the data much better than the one-factor model, which I expected since I wrote four of the 10 items with the two factors in mind for this part of the study. A comparison of the fit indices is below in Table 2.

Table 2

Comparison of the four models tested with confirmatory factor analysis

Model	χ^2	df	p	RMSEA	CFI	TLI	SRMR
6-item 1-factor	105.86	9	0.00	0.15	0.74	0.57	0.09
6-item correlated 2-factor	39.15	8	0.00	0.09	0.92	0.84	0.06
10-item 1-factor	846.87	35	0.00	0.28	0.52	0.39	0.23
10-item correlated 2-factor	75.90	34	0.00	0.07	0.98	0.97	0.05

The improved model fit indices of the 10-item correlated two-factor model were above commonly established rule-of-thumb thresholds (e.g. CFI > 0.95, TLI > 0.95). Furthermore, the factor loadings indicated the items loaded well on their respective factor (ranging from 0.55 to 0.90) and are detailed in Table 3. With excellent factor structure and fit indices indicating the two-factor model fit the data well, I concluded the Cybersecurity Attitudes Scale was ready to administer to a new sample of participants for the second phase of this research.

Table 3

Factor loadings for the correlated 2-factor model

Factor	Item	Loading
Policy Adherence	1	0.55
Policy Adherence	2	0.83
Policy Adherence	3	0.85
Policy Adherence	4	0.85
Policy Adherence	5	0.86
Perceived Vulnerability	6	0.71
Perceived Vulnerability	7	0.84
Perceived Vulnerability	8	0.90
Perceived Vulnerability	9	0.79
Perceived Vulnerability	10	0.72

Chapter 5
Study 3 – Modeling Cybersecurity Attitudes and Behavior

The two primary goals for this phase of my research are to test a model of the relationship between personality facets, cybersecurity attitudes (i.e. cyber policy adherence and perceived vulnerability), cybersecurity climate, perceived behavioral control, and cybersecurity behavior, and to determine whether this model is equivalent across two independent populations. Recently, organizations have put an emphasis on hiring cybersecurity and highly technical employees, especially in the private sector (Bergal, 2015). While many different occupations involve computer use and many are technical by nature, I am interested if differences exist between workers whose job it is to protect an organization's data and other occupations. Recently, Martin's (2017) study found work experience with computers to be a significant predictor of optimal cybersecurity behavior, with 8.5% of her sample currently working or previously working as cybersecurity / information security (IS) workers. However, all employees of an organization can be targeted using social engineering techniques, thus I tested whether there are measurement differences in the proposed model fit between cybersecurity / IS employees and non-cybersecurity / IS employees.

Method

Measures

Personality

Each of the 9 facets hypothesized to have a relationship with cybersecurity attitudes were measured using the 10-item International Personality Item Pool (IPIP) scales based on the NEO facets available at http://ipip.ori.org/newNEOFacetsKey.htm (Goldberg, 1999; Appendix B). The 9 facets measured were Order, Dutifulness, Self-Discipline, Deliberation, Altruism, Compliance, Fantasy, Ideas, and Positive Emotions. The reliability of the 10 NEO-based facet scales range from $\alpha = 0.71$ to $\alpha = 0.88$. Additionally, the Big Five personality factors (Extraversion, Conscientiousness, Openness-to-Experience, Agreeableness, and Neuroticism) were measured using the 10-item IPIP Big-Five Factor Markers short scales available at http://ipip.ori.org/newBigFive5broadKey.htm (Goldberg, 1999; Appendix C).

Cybersecurity Attitudes

Cybersecurity Attitudes were measured using the 10-item instrument (Appendix C) that was developed in phase one of this research. The scale measured two facets of cybersecurity attitudes: cyber policy adherence and perceived vulnerability. Item reliability analysis was conducted on the two facets separately, with the five items for policy adherence showing acceptable internal consistency reliability ($\alpha = 0.80$) in this sample, as did the five items for perceived vulnerability ($\alpha = 0.86$).

Cybersecurity Climate

Cybersecurity climate was measured using the 11-item instrument developed by Kessler et al. (under review; Appendix E). The survey included items for the following three climate areas: practices, values, and laxness. The internal consistency reliability of the instrument in this study was $\alpha = 0.82$. A sample item from the scale is "Issues related to the protection of private data are discussed in my workplace." I obtained permission to use the scale in this research from the first author.

Safety Climate

Safety climate was measured using the NIOSH short scale for measuring safety climate (Hahn & Murphy, 2008; Appendix F). The internal consistency reliability of the instrument was $\alpha = 0.87$ in this study. A sample item from the scale is “The health and safety of workers is a high priority with management where I work.”

Locus of Control

Locus of control was measured by a 3-item perceived behavioral control scale (Appendix G) that was adapted from Rotter (1966). (Workman, Bommer, and Straub, 2008). The scale exhibited high internal consistency reliability ($\alpha = 0.88$) in prior studies, however, in this study the internal consistency reliability was quite low ($\alpha = 0.61$). A sample item from this scale is “The primary responsibility for protecting my confidential information belongs to myself.”

Cybersecurity Behaviors

Cybersecurity behaviors was measured using a scale that was adapted from Hearth and Rao’s (2009) 3-item scale that measures cybersecurity intentions (Appendix H). The original scale exhibits excellent psychometric properties, as the factor loadings of the three items ranged from 0.87 to 0.94. In this study, the internal consistency reliability of the adapted scale was $\alpha = 0.90$.

Attention Check

The following question was used as an attention check for this study. "Recent research on decision making shows that choices are affected by context. Differences in how people feel, their previous knowledge and experience, and their environment can affect choices. To help us understand how people make decisions, we are interested in information about you. Specifically, we are interested in whether you actually take the time to read the directions; if not, some results may not tell us very much about decision making in the real world. To show that you have read the instructions, please ignore the question below about how you are feeling and instead check the "None of the above" option as your answer." This attention check was placed in the survey battery in the middle of the personality variables in an effort to best hide its proper usage.

Procedure

I collected data from two independent samples, cybersecurity / IT workers and non-IT workers. I recruited participants for the two samples through Amazon's Mechanical Turk (MTurk). MTurk has premium qualifications available for researchers to specialize the type of participants they want to use. For the IT worker sample, the premium qualification "employment status – software and information technology" was added as a prerequisite to participate in the study. Once this sample was collected, these MTurk workers were excluded from participating again in this research, as I blocked all participants from retaking the Mturk survey. The second sample was then collected by removing the premium qualification. All participants were limited to those currently employed and those who stated they are aware that their organization has information security / cybersecurity policies in place.

The participants were informed prior to taking the study that the research was anonymous with no linking information to their identity. The survey battery the participants completed asked them to provide the following demographics information: gender, age, race, annual income. The participants were then asked to complete the assessment battery consisting of the measures listed above (Appendix C-I). The total time necessary to take the study was approximately 15-20 minutes. I was able to take the study in six minutes by going as fast as possible while still reading the items. Therefore, I made the decision *a priori* to exclude all participants who finished the survey in under six minutes (though they were still compensated for participating if they did not fail the manipulation check). The participants were each paid $1.25 for participating. In determining a necessary sample size for a study that uses structural equation modeling, it is important to examine how many measured variables, latent variables, and free parameters are present in the model being tested. In my full model, there is a total of 122 measured variables and 15 latent variables. MacCallum, Browne, and Sugawara (1996) present a table to determine the sufficient sample size necessary to achieve desired power. For a study with at least 100 degrees of freedom, a sample size of 200 is sufficient for both measures of exact fit (power = .904) and close fit (power = .955). Since the models that will be examined in this study all have far more than 100 degrees of freedom, I proposed a sample of 200 participants for each of the two populations (IT vs. non-IT), for a total of 400 participants.

Participants

A total of 433 participants were recruited through MTurk. Prior to data analysis, a total of 56 participants were removed because they either stated that they were unemployed, or they finished the entire survey battery in less than six minutes. The participants were also presented with the attention check question similar to the question used in Martin (2017). This question asked about the participants' emotions, but at the end of the question stem stated to choose "none of the above". Only one participant failed the attention check, and this participant also finished in less than 6 minutes. This left a total of 377 participants for data analysis.

One item asked the participants for their job title, and after confirming they were either an IT or related job or not, there were 193 IT-related / software workers and 184 non-IT workers. There were 209 (55.4%) male participants and 166 (44%) female participants, with one participant choosing "other", but declining to specify, and one not answering. The average age of the participants was 37.78 years (SD = 11.71). The majority of the participants were full-time workers (n = 312, 82.8%). The participants were highly educated, with 71.1% (n = 268) having completed post-high school education, including 199 (53%) that completed at least a 4-year undergraduate degree. The annual household income of the participants varied quite a bit, with 40 (10.6%) earning under $25,000 annually, 115 (30.5%) earning between $25,000 and $49,999, 102 (27.1%) earning between $50,000 and $74,999, 47 (12.5%) earning between $75,000 and $99,999, 44 (11.7%) earning between $100,000 and $150,000, 15 (4.0%) earning over $150,000, and 14 (3.7%) preferring to not state their income. The participants were highly technically proficient, as they were asked to “please indicate your level of proficiency with computers and the Internet, and not a single person chose “very little to no proficiency”, while 91.5% (n = 345) indicated they were either “very proficient” or “extremely proficient”. Furthermore, 79.6% (n = 300) of the participants had “definitely” helped someone fix a computer.

Results

The first 5 hypotheses of this research were related to examining the bivariate relationship between personality facets and cybersecurity attitudes. When first hypothesized, the personality facets were theorized to have a relationship with overall cybersecurity attitudes. Since the structure of the cybersecurity attitudes instrument was shown to reflect two factors, the bivariate correlations of the personality facets were measured with both cyber policy adherence and perceived vulnerability, and if the expected relationship was significant between a facet and both attitudes then the hypothesis was deemed fully supported. If the facet had a significant relationship with only one attitude then the hypothesis was deemed partially supported, and if no significant relationship existed then the hypothesis was considered not supported. The two cybersecurity attitudes factors (i.e. policy adherence and perceived vulnerability) were significantly positively correlated ($r = 0.28$, $p < 0.01$).

Orderliness was positively related to policy adherence (r = 0.18, p < 0.01), but not significantly related to perceived vulnerability (r = 0.06, p = 0.23), therefore hypothesis 1A was partially supported. Dutifulness was positively related to both policy adherence (r = 0.45, p < 0.01) and perceived vulnerability (r = 0.20, p < 0.01), therefore hypothesis 1B was fully supported. Self-discipline was positively related to both policy adherence (r = 0.27, p < 0.01) and perceived vulnerability (r = 0.12, p < 0.05), therefore hypothesis 1C was fully supported. Deliberation was positively related to both policy adherence (r = 0.26, p < 0.01) and perceived vulnerability (r = 0.13, p < 0.05), therefore hypothesis 1D was fully supported. Overall, three of the four conscientiousness facets that were hypothesized to have a positive relationship with cybersecurity attitudes did in fact have that relationship with both cybersecurity attitudes factors, and the one that did not (i.e. orderliness) did have a positive relationship with policy adherence. These results provide support that there is a positive relationship between the hypothesized facets of conscientiousness and cybersecurity attitudes. However, it is interesting that there was a stronger relationship between all four conscientiousness facets and policy adherence than with perceived vulnerability (see table 4).

Table 4.
Correlations of Conscientiousness Facets with Cybersecurity Attitudes Factors

	Policy Adherence	Perceived Vulnerability
Orderliness	.18**	.06
Dutifulness	.45**	.20**
Self-Discipline	.27**	.12*
Deliberation	.26**	.13*

Note: * = p < 0.05, ** = p < 0.10

When examining the facets of agreeableness, altruism was positively related to both policy adherence (r = 0.38, p < 01) and perceived vulnerability (r = 0.13, p < 0.05), therefore hypothesis 2A was fully supported. Compliance was also positively related to policy adherence ($r = 0.36$, $p < 0.01$) and perceived vulnerability ($r = 0.12$, $p < 0.05$), therefore hypothesis 2B was fully supported. These results provide support that there is a positive relationship between the hypothesized facets of agreeableness and cybersecurity attitudes.

Fantasy was not related to either policy adherence ($r = 0.08$, $p = 0.12$) or perceived vulnerability ($r = 0.09$, $p = 0.09$), therefore hypothesis 3A was not supported. Intellect (Ideas) was positively related to both policy adherence ($r = 0.27$, $p < 0.01$) and perceived vulnerability ($r = 0.14$, $p < 0.01$), therefore hypothesis 3B was fully supported. I obtained mixed results regarding the facets of openness-to-experience that I hypothesized would relate to cybersecurity attitudes. Positive emotions were positively related to policy adherence ($r = 0.14$, $p < 0.01$), but not significantly related to perceived vulnerability (0.08, $p = 0.15$). Therefore, hypothesis 4 was only partially supported.

The relationship between cybersecurity attitudes and cybersecurity behaviors was interesting, as there was a strong positive relationship between policy adherence and cybersecurity behaviors ($r = 0.56$, $p < 0.01$), and a positive, though much smaller, relationship between perceived vulnerability and cybersecurity behaviors ($r = 0.20$, $p < 0.01$). With both relationships being significantly positive, hypothesis 5 was fully supported. However, it is notable that the magnitude of the relationships is quite different. Cybersecurity climate and cybersecurity behaviors were strongly positively related ($r = 0.58$, $p < 0.01$), providing support for hypothesis 6; while internal locus of control was also positively related to cybersecurity behaviors ($r = 0.41$, $p < 0.01$) providing support for hypothesis 7.

Regarding research question 1, there was a strong correlation between safety climate and cybersecurity climate ($r = 0.56$, $p < 0.01$). While these constructs are related, I would interpret this correlation as support that the variables are not the same construct, but it does appear that the cybersecurity climate construct is strongly related to safety climate in the manner the two constructs are currently being measured. Furthermore, the two constructs seem to be similarly related to criterion variables, as cyber climate was positively related to cybersecurity behaviors ($r = 0.58$, $p < 0.01$), while safety climate was also strongly related to cybersecurity behaviors ($r = 0.46$, $p < 0.01$).

The structural model (figure 3) that I expected to have the best fit was tested in MPlus 7.3 (Muthén & Muthén, 1998-2012). Regarding exogenous variables, dutifulness, compliance, and altruism were negatively skewed and had high values of kurtosis, and for endogenous variables, cybersecurity behaviors were highly negatively skewed (see table 5).

Table 5.

Descriptives of study's variables

Variable	Mean	SD	Min	Max
Cyber Adherence Policy	23.02	2.56	11	25
Perceived Vulnerability	20.07	4.24	5	25
Cybersecurity Climate	42.40	7.26	21	55
Orderliness	37.92	7.91	11	50
Dutifulness	43.10	5.31	22	50
Self-Discipline	37.31	8.63	10	50
Deliberation	38.83	7.30	16	50
Altruism	41.07	6.44	15	50
Compliance	40.57	6.91	12	50
Fantasy	37.12	8.34	10	50
Intellect	39.93	7.41	10	50
Positive Emotions	36.84	7.98	10	50
Locus of Control	11.52	2.35	3	15
Cybersecurity Behaviors	13.63	1.94	5	15

Variables with high kurtosis values and non-normality are particularly problematic in structural equation modeling, thus, Satorra-Bentler corrections were used in the structural equation modeling analysis. This is performed by using the "Estimator = MLM" and "Listwise = on" commands in MPlus. This correction provides robust estimates of the CFI, TLI, and RMSEA regardless of non-normality (Byrne, 2012; p. 100). One consideration when using the Satorra-Bentler correction is that the chi-square value cannot be interpreted in the same manner and cannot be used for traditional chi-square difference testing. The model fit indices for the original model are as follows: χ^2 = 14,871.11, df = 6592, p = 0.00, RMSEA = 0.06 [0.059, 0.061], CFI = 0.68, TLI = 0.67, SRMR = 0.09. These results indicate the model is a poor fit for the data, especially with such low values for the CFI and TLI. This model with only the significant beta and gamma weight paths obtained from this analysis is displayed in Figure 4.

Many of the paths that represented significant bivariate correlations became non-significant in this analysis. Furthermore, deliberation and positive emotion had a negative relationship with policy adherence in this model and compliance had a negative relationship with perceived vulnerability after having a positive relationship when examining correlations separately. Furthermore, there was not a significant path from perceived vulnerability to cyber behaviors, and only two conscientiousness paths (orderliness and dutifulness) were significant in this model. Figure 5 displays the alternative model, which has a path going from locus of control to policy adherence and perceived vulnerability instead of cybersecurity behaviors. This model was based on the non-significant path in Ajzen's (1985) original model. This model also was a poor fit for the data, with nearly identical fit indices to the original hypothesized model: χ^2 = 14,581.22, df = 6591, p = 0.00, RMSEA = 0.06 [0.058, 0.061], CFI = 0.68, TLI = 0.67, SRMR = 0.09.

Model assessment was then conducted on the models exchanging the personality facets for the four factors that housed the facets: extraversion, agreeableness, conscientiousness, and openness-to-experience. Contrary to the *a priori* expected results, the model had some better fit indices (i.e. CFI and TLI) than by measuring using the facets. The fit indices for this model are as follows: $\chi^2 = 4804.55$, df = 1679, p = 0.00, RMSEA = 0.07 [0.068, 0.073], CFI = 0.78, TLI = 0.77, SRMR = 0.08. Though the model fit the data poorly, the CFI and TLI were improved over the model based on personality facets. An exploratory model using just conscientiousness and agreeableness as factors predicting policy adherence attitudes and perceived vulnerability had the best CFI and TLI among models tested: $\chi^2 = 2898.02$, df = 842, p = 0.00, RMSEA = 0.08 [0.077,0.083], CFI = 0.79, TLI = 0.77, SRMR=0.09; though this model still exhibits poor fit.

Though the hypothesized model was a poor fit for the data, as was the alternative model, one of the goals of this research was to test the measurement invariance of the proposed models. Keeping in mind that several variables are non-normal, that there is multivariate non-normality, and that the model has poor fit, I still examined configural invariance in the hypothesized model. The first attempt was using MLM as the estimator and there was no convergence. Further testing using maximum likelihood as the estimator was conducted, and again there was no convergence.

Exploratory Results

Because the hypothesized model and the alternative model that incorporated personality facets were both poor fit for the data and the configural measurement invariance test would not converge, I decided to conduct exploratory analysis on the data. First, I tested removing all the personality facets from the model except for the conscientiousness facets to examine how the fit indices would change. Since conscientiousness has been found to be significantly related to many organizational behaviors such as job performance (Barrick & Mount, 1991), interpersonal and organizational deviance (Berry, Ones, & Sackett, 2017), and cooperative behavior in the workplace (LePine & Van Dyne, 2001), I left the conscientiousness facets in the model because they make the most sense conceptually to be related to cybersecurity attitudes, especially with policy adherence. Using MLM as the estimator, the model fit indices were as follows: $\chi^2 =$

5749.67, df = 2117, p = 0.00, RMSEA = 0.07 [0.066, 0.071], CFI = 0.73, TLI = 0.72, SRMR = 0.09. These fit indices signal that this is still a poor fit for the data.

Next, I removed the personality facets completely from the model, and conducted an analysis on only the cyber analogs to the theory of planned behavior (minus intentions). This model still exhibited poor fit indices, and less fit than keeping the conscientiousness facets in the model: χ^2 = 1567.82, df = 314, p = 0.00, RMSEA = 0.10 [0.099, 0.109], CFI = 0.70, TLI = 0.67, SRMR = 0.10. This model was a poor fit for the data, and further examination of the modification indices showed that there were several residuals among the cybersecurity climate scale that were exceptionally high (e.g., 150-200). There is no theoretical justification for correlating residuals, therefore I left the model as is, but it was informative seeing the modification indices with a manageable number in the MPlus output. Next, I aggregated the items for each variable and ran a path analysis on the "measured" variables. This model had the worst fit of all the models: χ^2 = 123.11, df = 14, p = 0.00, RMSEA = 0.15 [0.13, 0.17], CFI = 0.73, TLI = 0.32, SRMR = 0.06.

Lastly, I standardized all of the individual items to z scores and conducted structural equation modeling analysis on the transformed scores, using MLM for an estimator and only allowing the personality facets to be correlated with other facets in their respective factor. Some of the model fit indices (e.g. CFI and TLI) were slightly improved from the hypothesized model, but overall this model was still a poor fit for the data: χ^2 = 11011.43, df = 5087, p = 0.00, RMSEA = 0.06 [0.062, 0.066], CFI = 0.75, TLI = 0.74, SRMR = 0.11.

Table 6.
Model Fit Indices for All Models Tested in Analysis

	χ^2	df	RMSEA	RMSEA CI	CFI	TLI	SRMR
Hypothesized Models							
Full Model	14,871.11	6592	0.06	[.059, .061]	0.68	0.67	0.09
Alternative Model	14,851.22	6591	0.06	[.058, .061]	0.69	0.68	0.09
Factors Model	4804.55	1679	0.07	[.068, .073]	0.78	0.77	0.08
Exploratory Models							
Factors (Con&Agree)	2898.02	842	0.08	[.077, .083]	0.79	0.77	0.09
Con Facets Only	5749.67	2117	0.07	[.066, .071]	0.73	0.72	0.09
No Personality	1567.82	314	0.10	[.099, .109]	0.70	0.67	0.10
Path Analysis	123.11	14	0.15	[.13, .17]	0.73	0.32	0.06
Z Scores	11,011.43	5087	0.06	[.062,.066]	0.75	0.74	0.11

Note: Con = Conscientiousness, Agree = Agreeableness

Chapter Six
Discussion

There were two parts to this study – the development of the cybersecurity attitudes scale, and the examination of the relationship the cybersecurity attitudes construct has with other variables by examining the bivariate correlations between the study's variables, and then in the context of a structural model. Through a three-step iterative process, I was able to develop an instrument to measure cybersecurity attitudes. While the intent of this research at the outset was to examine general cybersecurity attitudes, results of the administration of the initial instrument (Appendix A) suggested that there were two factors being measured. Examining the items that loaded on the two factors indicated that the factors being measured were cyber policy adherence attitudes and perceived vulnerability to a cyberattack. After two subsequent administrations of revised versions of the Cybersecurity Attitudes Scale, a finalized version of the scale displaying good psychometric properties remained (i.e. Cronbach's alpha greater than 0.80 and all factor loadings on respective factors greater than 0.50).

Minimizing or eliminating risky employee cybersecurity behaviors is a priority for organizations in today's work environment. Development of a scale that measures employees' attitudes regarding cybersecurity could be considered a key practical step in assisting organizations attempting to ameliorate cyber behaviors that have negative consequences. Broadly speaking, there is a plethora of empirical evidence that support the view that attitudes can predict future behavior (e.g., Kraus, 1995), and this relationship between attitudes and behavior has been shown to also be true in the organizational sciences (e.g., the relationship between turnover intentions resulting from disaffect with an employer and subsequent turnover; Vanderberg & Nelson, 1999). Thus, the CAS can have practical benefits for organizational researchers seeking to better understand why employees continue to behave in ways that put an organization's data at risk.

The positive bivariate correlations that many of the personality facets have with cyber policy adherence attitudes and perceived vulnerability support further examination of the relationship between these facets and cyber attitudes. However, the results of this study appear to indicate that the relationship between personality facets and attitudes differ whether you examine the policy adherence relationship or the perceived vulnerability relationship. The two attitudinal factors positively correlated with each other ($r = 0.28$, $p < 0.01$). However, that relationship is small enough to suggest that while they are certainly related, they might be different attitudes. As mentioned above, the conscientiousness facets (i.e. orderliness, dutifulness, self-discipline, and deliberation) were all correlated more strongly with policy adherence than perceived vulnerability (see table 4).

These results may help explain why Dreibelbis (2016) found a relationship between conscientiousness and cyber misbehavior, Hu et al. (2012) found a relationship between dutifulness and cybersecurity intentions, and Martin (2017) was unable to find a significant relationship between conscientiousness and cybersecurity behavior. Following the results of Hu et al. (2012), this research found the dutifulness facet to have the strongest relationship with both cybersecurity attitudes. On the other hand, orderliness had a much smaller relationship with policy adherence than dutifulness and had no significant relationship with perceived vulnerability. If the conscientiousness items that measured the orderliness, competence, and achievement-striving were attenuating the relationship with cybersecurity behaviors, that could account for the reason Martin (2017) had difficulty obtaining results similar to Dreibelbis (2016). Perhaps solely measuring the conscientiousness facets that have the strongest relationships with attitudes, intentions, and behavior would be a fruitful next step for researchers to take.

The structural equation model hypothesized to be the best fit for the data was not plausible, nor were any of the alternative models. There may be a couple of reasons why these models were a poor fit for the data. The first reason is there was barely any variance in the cybersecurity behavior variable (the right-most endogenous variable in the model), as 56.2% ($n = 212$) chose "strongly agree" with all 3 items on the scale. This variable had a skewness of -1.54 (standard error = 0.13) and a kurtosis of 2.30 (standard error = 0.25). Furthermore, several exogenous variables (i.e. dutifulness, compliance, altruism) were also negatively skewed.

I suspect that some of the negative skew of these variables occurred due to the use of MTurk workers for this study. The MTurk workers were extremely technically proficient and were also a highly conscientious and agreeable sample. I think it is quite possible there would be a lot more variance in the study's variables if an organizational sample of workers was used to conduct the research. Another possible method to combat the "socially desirable" answers would have been to administer a social desirability scale with the survey battery. Though it is possible that professional survey participants know how to respond to social desirability scales as well since they make income from participating in survey research.

Likewise, I should have had multiple attention checks. The attention check used in this research was based on the one used in the Martin (2017) study. However, Martin (2017) had a sizable percentage (roughly 10%) of participants fail the attention check, while I only had one participant answer the attention check incorrectly. Another limitation of this study was the study design. The hypothesized models in this study suggest that cybersecurity attitudes mediates the relationship between personality facets and cybersecurity behaviors. However, the study was a cross-sectional design, with self-report survey data collected at only one timepoint. To truly test for mediating effects, a researcher would want to use a longitudinal design to better understand causal effects.

Conclusion

Cybersecurity misbehaviors are having an increasingly costly effect on present-day organizations and understanding the mechanisms underlying why employees continue to have suboptimal cybersecurity behaviors is an important research domain. This study adds to the extant literature in the nascent cybersecurity and industrial-organizational psychology domain with the development of a scale that researchers can use to measure an individual’s cybersecurity attitudes across two dimensions: cyber policy adherence attitudes and perceived vulnerability to a cyberattack. The three-step iterative process using independent samples resulted in a scale that displays good psychometric properties. The resultant Cybersecurity Attitudes Scale is of practical use to academic researchers and hopefully to organizations as well. This research also found there to be a strong bivariate relationship between cyber policy adherence attitudes and dutifulness, altruism, compliance and cybersecurity climate. The bivariate relationship between perceived vulnerability and these variables was significant, but to a lesser degree, so future research may want to examine how personality factors and/or facets differentially predict different cybersecurity attitudes and subsequent intentions and behaviors. Finally, the hypothesized models of personality facets, attitudes, climate, locus of control, and behavior exhibited poor fit for the data collected in this sample. However, future research using an organizational sample, or a sample that has a large amount of variance in this study’s variables may find more support for the hypothesized models used in this study.

References

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, 32(3), 183-196.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior (pp. 11-39). Springer Berlin Heidelberg.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211.

Allport, G. W., & Odbert, H. S. (1936). Trait-names: A psycho-lexical study. *Psychological Monographs*, 47 (1, Whole No. 211).

Anderson, C. (2005). Creating conscientious cybercitizen: an examination of home computer user attitudes and intentions towards security, Presented at Conference on Information Systems Technology (CIST)/INFORMS, 2005, San Francisco, California

Arena, C. (2014, August 13). 4 Reasons Why Exponential Technologies Are Taking Off. Retrieved November 19, 2015.

Ashton, K. (2009). That 'internet of things' thing. RFiD Journal, 22(7), 97-114.

Barenbaum, N. B., & Winter, D.G. (2008). History of modern personality theory and research. Handbook of Personality: Theory and Research, 3-28.

Barker, R. G. (1965). Explorations in ecological psychology. *American Psychologist*, 20(1), 1.

Barrett, D., Yadron, D., & Paletta, D. (2015). U.S. suspects hackers in China breached about 4 million people's records, officials ssay. Retrieved November 20, 2015, from http://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888

Barrick, M. R., & Mount, M. K. (1991). The Big Five personality dimensions and job performance: A meta-analysis. *Personnel Psychology*, 44, 1-26.

Beck, L., & Ajzen, I. (1991). Predicting dishonest actions using the theory of planned behavior. *Journal of Research in Personality*, 25(3), 285-301.

Bergal, J. (2015). Hiring cybersecurity staff is hard for states. Retrieved November 25, 2015, from http://www.govtech.com/security/Hiring-Cybersecurity-Staff-Is-Hard-for-States.html

Berry, C. M., Ones, D. S., & Sackett, P. R. (2007). Interpersonal deviance, organizational deviance, and their common correlates: A review and meta-analysis. *Journal of Applied Psychology*, 92(2), 410.

Bilker, W. B., Hansen, J. A., Brensinger, C. M., Richard, J., Gur, R. E., & Gur, R. C. (2012). Development of abbreviated nine-item forms of the Raven's Standard Progressive Matrices Test. Assessment, 19(3), 354-369.

Bort, J. (2014). How the hackers broke into Sony and why it could happen to any company. Retrieved November 28, 2015, from http://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12

Briggs, B., & Shingles, M. (2015). Tech Trends 2015, Exponentials. Retrieved May 01, 2016, from http://dupress.com/articles/tech-trends-2015-exponential-technologies/

Burke, M. J., Borucki, C. C., & Kaufman, J. D. (2002). Contemporary perspectives on the study of psychological climate: A commentary. *European Journal of Work and Organizational Psychology,* 11, 325– 340.

Byrne, B. M. (2012). Structural equation modeling with Mplus. [electronic resource]: basic concepts, applications, and programming. New York : Routledge, 2012.

Cattell, R. B. (1943). The description of personality: Basic traits resolved into clusters. *The Journal of Abnormal and Social Psychology*, 38(4), 476-506. doi:10.1037/h0054116

Cattell, R. B. (1963). Theory of fluid and crystallized intelligence: A critical experiment. *Journal of Educational Psychology*, 54(1), 1.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, *1*(3), 18-41.

Coovert, M. D., & Goldstein, M. (1980). Locus of control as a predictor of users' attitude toward computers. *Psychological Reports*, 47(3_suppl), 1167-1173.

Costa, P. T, Jr., & McCrae, R. R. (1992). Four ways five factors are basic. Personality and Individual Differences, 13, 653-665.

Costa, P. T, Jr., & McCrae, R. R. (1992). Revised NEO Personality Inventory (NEO-PI-R) and NEO Five-Factor Inventory (NEO-FFI) manual. Odessa, FL: Psychological Assessment Resources.

Denison, D. R. (1996). What is the difference between organizational culture and organizational climate? A native's point of view on a decade of paradigm wars. *Academy of Management Review*, 21(3), 619-654.

DeYoung, C. G., Peterson, J. B., & Quilty, L. C. (2007). Between facets and domains: 10 aspects of the Big Five. *Journal Of Personality and Social Psychology*, (5), 880.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2006). User behavior toward preventive technologies–cultural differences between the United States and South Korea.

Dorsey, D. W., Martin, J., Howard, D. J., & Coovert, M. D. (2017). Cybersecurity issues in selection. In Farr, J. L. & Tippins, N. T. (Eds.), Handbook of employee selection (pp. 913–930). New York, NY: Routledge

Dreibelbis, R. (2016). It's more than Just Changing Your Password: Exploring the Nature and Antecedents of Cyber-Security Behaviors.

Ehrhart, M. G., & Raver, J. L. (2014). The effects of organizational climate and culture on productive and counterproductive behavior. The Oxford handbook of organizational climate and culture, 153-176.

Ehrhart, M. G., Schneider, B., & Macey, W. H. (2014). Organizational climate and culture: an introduction to theory, research, and practice. New York, NY : Routledge, 2014.

Erbschloe, M. (2005). Trojans, worms, and spyware. [electronic resource] : a computer security professional's guide to malicious code. Amsterdam : Boston : Elsevier Butterworth Heinemann, c2005.

Eysenck, H. J. (1991). Dimensions of personality: 16, 5, or 3? Criteria for a taxonomic paradigm. *Personality and Individual Differences*, 12, 773-790.

Fiske, D. W. (1949). Consistency of the factorial structures of personality ratings from different sources. *Journal of Abnormal and Social Psychology*, 44, 329-344.

Fishbein, M., & Ajzen, I. (1974). Attitudes towards objects as predictors of single and multiple behavioral criteria. Psychological Review, 81, 59–74.

Gazica, M. W., & Spector, P. E. (2016). A test of safety, violence prevention, and civility climate domain-specific relationships with relevant workplace hazards. *International Journal of Occupational and Environmental Health,* 22(1), 45-51.

Goldberg, L. R. (1993). The structure of phenotypic personality traits. *The American Psychologist*, (1), 26.

Goldberg, L. R. (1999). A broad-bandwidth, public domain, personality inventory measuring the lower-level facets of several five-factor models. In I. Mervielde, I. Deary, F. De Fruyt, & F. Ostendorf (Eds.), *Personality Psychology in Europe*, Vol. 7 (pp. 7-28). Tilburg, The Netherlands: Tilburg University Press.

Grant Thornton (2015). Cyber attacks cost global business over $300bn a year. Retrieved November 19, 2015, from http://www.grantthornton.global/en/insights/articles/cyber-attacks-cost-global-business-over-$300bn-a-year/

Greenberg, A. (2015). OPM now admits 5.6m Feds' fingerprints were stolen by hackers. Retrieved November 19, 2015, from http://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/

Griffin, M. A., & Neal, A. (2000). Perceptions of safety at work: a framework for linking safety climate to safety performance, knowledge, and motivation. *Journal of Occupational Health Psychology*, 5(3), 347.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

Guo, K. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security* 32, 242-251.

Guo K., Yuan Y., Archer N., Connelly C. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal Of Management Information Systems* 28(2):203-236.

Hahn, S. E., & Murphy, L. R. (2008). A short scale for measuring safety climate. *Safety Science*, 46(7), 1047-1066.

Hawk, S. R. (1989). Locus of control and computer attitude: The effect of user involvement. *Computers in Human Behavior*, 5(3), 199-206.

Hellriegel, D., & Slocum, J. W. (1974). Organizational climate: Measures, research and contingencies. *Academy of Management Journal*, 17(2), 255-280.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.

Hough, L. M., & Furnham, A. (2003). Use of personality variables in work settings. In W. Borman, D. Ilgen, & R. Klimoski (Eds.), Handbook of psychology (pp. 131–169). New York, NY: Wiley.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615-660.

John, O. P., Naumann, L. P., & Soto, C. J. (2008). Paradigm shift to the integrative Big Five trait taxonomy. Handbook of Personality: Theory and Research, 3, 114-158.

Johnson, J. W. (1996). Linking employee perceptions of service climate to customer satisfaction. *Personnel Psychology*, 49(4), 831-851.

Judge, T. A., Rodell, J. B., Klinger, R. L., Simon, L. S., & Crawford, E. R. (2013). Hierarchical representations of the five-factor model of personality in predicting job performance: Integrating three organizing frameworks with two theoretical perspectives. *Journal Of Applied Psychology*, (6), Kelly, E. (2015, June 27). OPM hack Q&A: What we know and what we don't. Retrieved November 17, 2015, from http://www.usatoday.com/story/news/politics/2015/06/27/opm-hack-questions-and-answers/29333211/

Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., & Spector P. E. (2016). Promoting cybersecurity within healthcare. Paper presented at the Academy of Management conference, Atlanta, GA, August 4-8.Kraus, S. J. (1995). Attitudes and the prediction of behavior: A meta-analysis of the empirical literature. Personality and social psychology bulletin, 21(1), 58-75.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2014). Advanced social engineering attacks. *Journal of Information Security and Applications* 10/2014, 22. DOI: 10.1016/j.jisa.2014.09.005

LePine, J. A., & Van Dyne, L. (2001). Voice and cooperative behavior as contrasting forms of contextual performance: evidence of differential relationships with big five personality characteristics and cognitive ability. *Journal of Applied Psychology*, 86(2), 326.

Likert, R. (1961). New patterns of management.

Litwin, G. H., & Stringer, R. A. (1968). Motivation and organizational climate. Cambridge, MA: Harvard Business School, Division of Research.

MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. *Psychological methods*, 1(2), 130.

Mathieson, K. (1991), ``Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior. *Information System Research*, Vol. 3 No. 2, pp. 173-91.

Martin, J. (2017) Something Looks Phishy Here: Applications of Signal Detection Theory to Cyber-Security Behaviors in the Workplace

Muthén, L.K. and Muthén, B.O. (1998-2012). Mplus User's Guide. Seventh Edition. Los Angeles, CA: Muthén & Muthén

Neal, A., & Griffin, M. A. (2004). Safety climate and safety at work. *The Psychology of Workplace Safety*, 15-34.

Patterson, M. G., West, M. A., Shackleton, V. J., Dawson, J. F., Lawthom, R., Maitlis, S., & Wallace, A. M. (2005). Validating the organizational climate measure: links to managerial practices, productivity and innovation. Journal of organizational behavior, 26(4), 379-408.

Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological monographs: General and applied*,*80*(1), 1.

Russell, M. T., Cattell, R. B., Cattell, A. K. S., Cattell, H. E., & Karol, D. L. (1994). 16PF Fifth Edition Administrator's manual. Institute for Personality and Ability Testing, Incorporated.

Schmidt, F. L., & Hunter, J. E. (1998). The validity and utility of selection methods in personnel psychology: Practical and theoretical implications of 85 years of research findings. *Psychological Bulletin*, 124(2), 262.

Schaller, R. R. (1997). Moore's law: past, present and future. *Spectrum, IEEE*,*34*(6), 52-59.

Schneider B., & Barbera K., (2014). The Oxford Handbook of Organizational Climate and Culture. Oxford, UK: Oxford Univ. Press

Schneider, B., Ehrhart, M. G., & Macey, W. H. (2011). Organizational climate research: achievements and the road ahead. In N. M. Ashkanasy, C. P. M. Wilderom, & M. F. Peterson (Eds.), Handbook of organizational culture and climate, 2nd ed. Thousand Oaks, CA: Sage.

Schneider, B., & Snyder, R. A. (1975). Some relationships between job satisfaction and organization climate. *Journal of Applied Psychology*, 60(3), 318.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31. doi:10.1108/09685220010371394

Spector, P. E. (1982). Behavior in organizations as a function of employee's locus of control. *Psychological Bulletin*, *91*(3), 482.

Spector, P. E. (1988). Development of the work locus of control scale. *Journal of Occupational Psychology*, 61(4), 335-340.

Symantec (2015). ISTR20 Internet Security Report. April 2015, Volume 20.

Thoresen, C. J., Kaplan, S. A., Barsky, A. P., Warren, C. R., & de Chermont, K. (2003). The affective underpinnings of job perceptions and attitudes: A meta-analytic review and integration. *Psychological Bulletin*, *129*(6), 914-945. doi:10.1037/0033-2909.129.6.914

Tupes, E. C, & Christal, R. E. (1961). Recurrent personality factors based on trait ratings (USAF ASD Tech. Rep. No. 61-97). Lackland Air Force Base, TX: U.S. Air Force.

Valcour, P. M., & Hunter, L. W. (2005). Technology, organizations, and work-life integration (pp. 61-84). na.

Vandenberg, R. J., & Nelson, J. B. (1999). Disaggregating the motives underlying turnover intentions: When do intentions predict turnover behavior?. *Human relations*, 52(10), 1313-1336.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799-2816.

Zengerle, P., & Cassella, M. (2015). Millions more Americans hit by government personnel data hack. Retrieved May 03, 2016, from http://www.reuters.com/article/us-cybersecurity-usa-idUSKCN0PJ2M420150709.

Zetter, K. (2014). Sony got hacked hard: What we know and don't know so far. Retrieved November 14, 2015, from http://www.wired.com/2014/12/sony-hack-what-we-know/

Zohar, D. (1980). Safety climate in industrial organizations: Theoretical and applied implications. *Journal of Applied Psychology*, 65(1), 96-102. doi:10.1037/0021-9010.65.1.96

Table 7. *Correlation Matrix of Study Variables* * = p < 0.05, ** = p < 0.01; n = 377

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1. Policy Adherence														
2. Perceive Vulnerability	.28**													
3. Orderliness	.18**	.06												
4. Dutifulness	.45**	.20**	.39**											
5. Self-Discipline	.27**	.12*	.52**	.54**										
6. Deliberation	.26**	.13*	.50**	.63**	.56**									
7. Altruism	.38**	.13*	.21**	.63**	.38**	.38**								
8. Compliance	.36**	.12*	.34**	.70**	.44**	.57**	.60**							
9. Fantasy	.08	.09	-.07	.04	-.10	-.08	.23**	-.01						
10. Intellect	.27**	.14**	.03	.30**	.19**	.16**	.33**	.18**	.40**					
11. Positive Emotions	.14**	.08	.18**	.28**	.38**	.07	.49**	.22**	.18**	.23**				
12. Cyber Behavior	.56**	.20**	.20**	.51**	.29**	.29**	.40**	.37**	.14**	.31**	.16**			
13. Cyber Climate	.53**	.20**	.11*	.40**	.32**	.26**	.41**	.36**	.08	.35**	.25**	.58**		
14. Locus of Control	.35**	.14**	.07	.31**	.26**	.23**	.22**	.21**	.01	.27**	.14**	.41**	.45**	

Figures

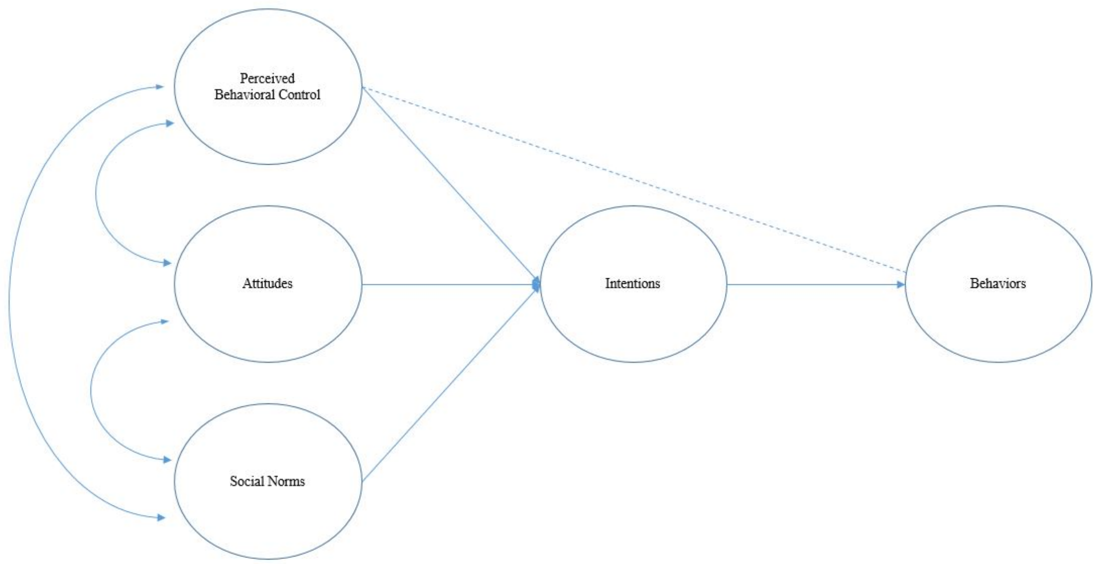

Figure 1: *Model of the theory of planned behavior.*

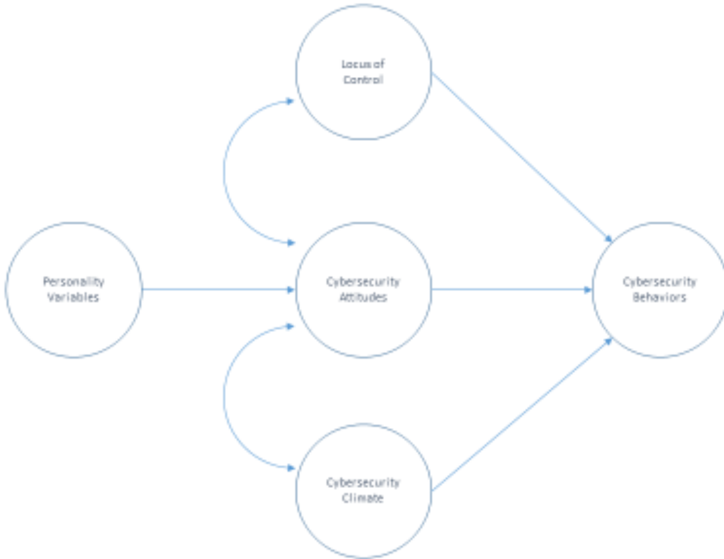

Figure 2: *Refined theory of planned behavior with cyber adaptation to variables.*

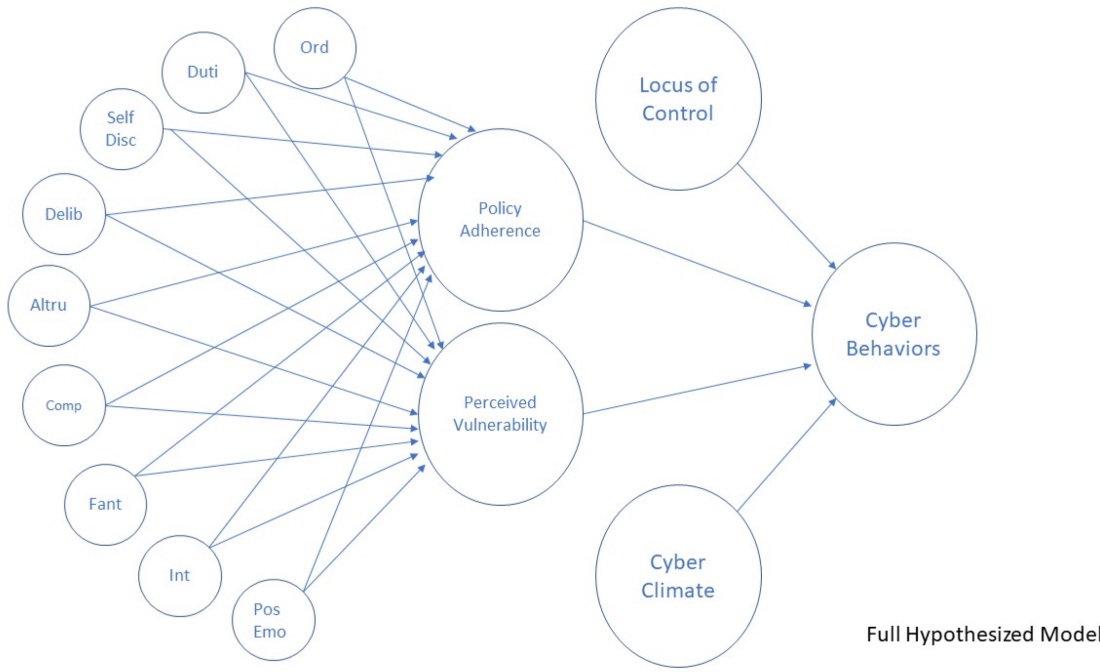

Figure 3: *Hypothesized Structural Model.*

Note: Personality facets will covary, paths not shown in picture for clarity.

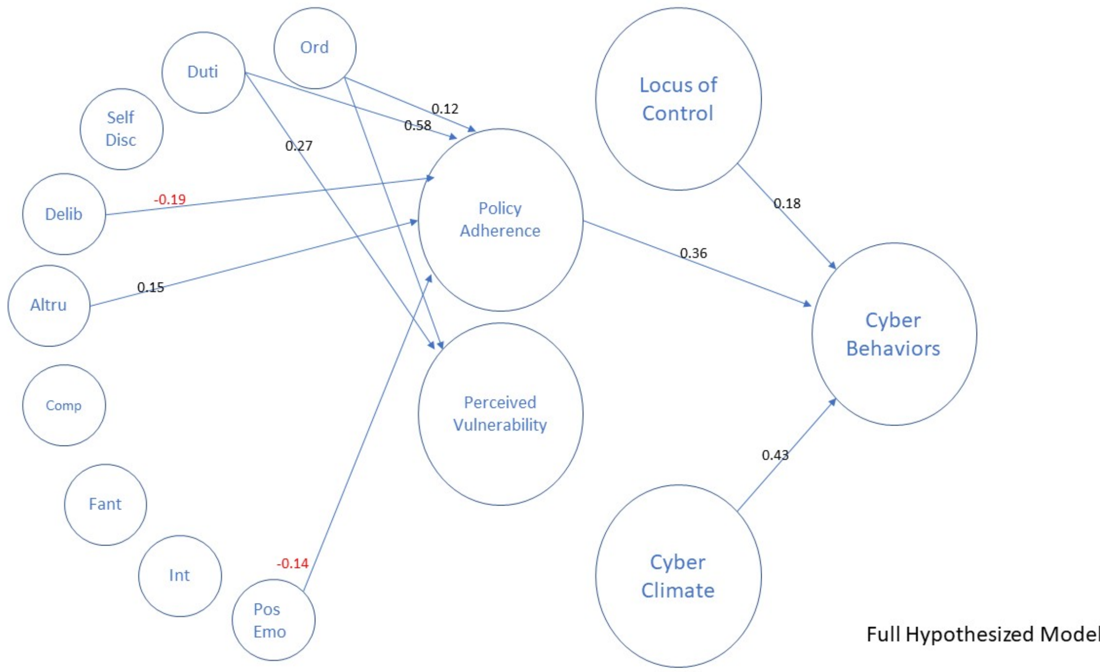

Figure 4: *Hypothesized Model with only Significant Paths in Model*

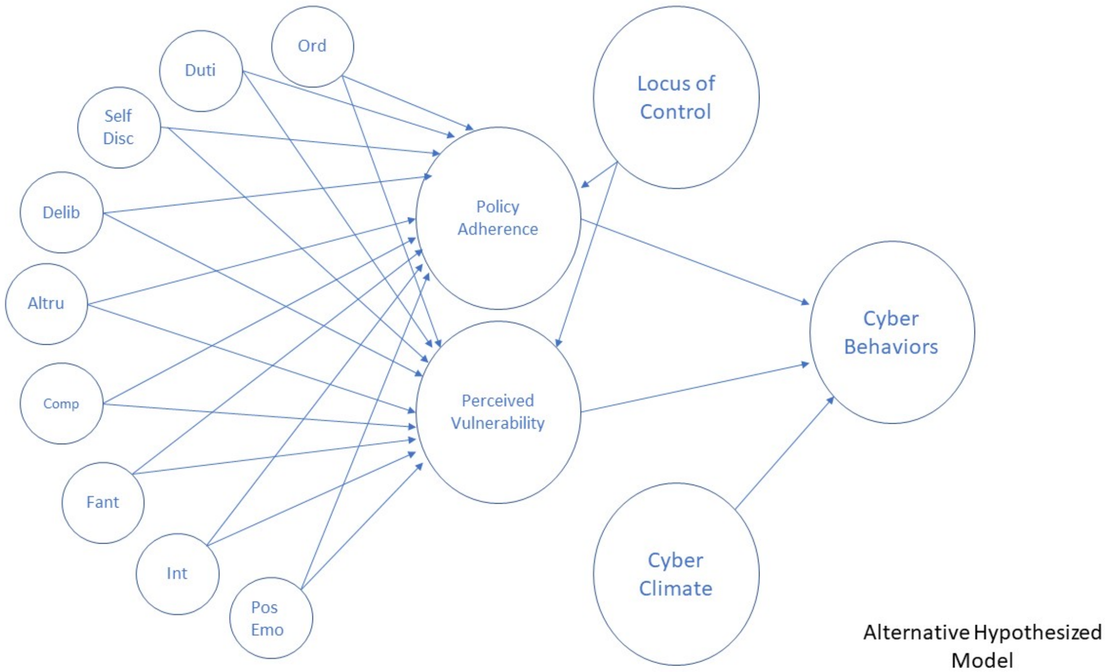

Figure 5: Alternative Hypothesized Model with LOC to Cybersecurity Attitudes

Appendices

Appendix A: Pilot Study Cybersecurity Attitudes Scale

Please answer on a scale of 1 (Strongly disagree) to 5 (Strongly agree) about how you feel the statement reflect your own views.

1. I feel it is necessary to use strong passwords for my applications at work.
2. I feel it is important to follow organizational cybersecurity policies.
3. I believe it is more important to get my work done in a timely fashion than to follow cybersecurity policies.
4. I feel it is important to never intentionally violate my organization's cybersecurity policies.
5. I feel all email attachments I receive at my work email address are safe to download.
6. I feel it is inconvenient to have different passwords at work for different applications.
7. I believe it is unlikely I could be a victim of a cyberattack at work.
8. I believe I am vulnerable to my personal confidential information being stolen from my organization in a cyberattack.

Appendix B: Cybersecurity Attitudes Scale Version 2

Please answer on a scale of 1 (Strongly disagree) to 5 (Strongly agree) about how you feel the statement reflect your own views.

1. I feel it is necessary to use strong passwords for my applications at work.
2. I feel it is important to follow organizational cybersecurity policies.
3. I feel it is important to never intentionally violate my organization's cybersecurity policies.
4. I feel all email attachments I receive at my work email address are safe to download.
5. I believe it is unlikely I could be a victim of a cyberattack at work.
6. I believe I am vulnerable to my personal confidential information being stolen from my organization in a cyberattack.

Appendix C: Cybersecurity Attitudes Scale (Final Version)

1. I feel it is necessary to use strong passwords for my applications at work.
2. I feel it is important to follow organizational cybersecurity policies.
3. I feel it is important to never intentionally violate my organization's cybersecurity policies.
4. I feel it is in my best personal interest to follow my organization's cybersecurity policies.
5. I feel it is in my employer's best interest to hire individuals who follow the organization's cybersecurity policies.
6. I feel it is possible I could receive a harmful email attachment at my work email address.
7. I feel it is possible that my organization could be the victim of a cyberattack.
8. I feel it is possible that I could be a victim of a cyberattack at work.
9. I feel it is possible that an employee browsing the internet could lead to a cyberattack at my organization
10. I feel I am vulnerable to my personal information being stolen from my organization in a cyberattack.

Appendix D: Personality Facets (NEO)

On the following page, there are phrases describing people's behaviors. Please use the rating scale below to describe how accurately each statement describes you. Describe yourself as you generally are now, not as you wish to be in the future. Describe yourself as you honestly see yourself, in relation to other people you know of the same sex as you are, and roughly your same age. So that you can describe yourself in an honest manner, your responses will be kept in absolute confidence.

Please read each statement carefully, and then select an option on the scale.
Response Options: 1 = "Very Inaccurate"; 2 = "Moderately Inaccurate"; 3 = "Neither Inaccurate nor Accurate"; 4 = "Moderately Accurate"; 5 = "Very Accurate"

Orderliness (.82)

+ keyed
    Like order.
    Like to tidy up.
    Want everything to be "just right."
    Love order and regularity.
    Do things according to a plan.

– keyed
    Often forget to put things back in their proper place.
    Leave a mess in my room.
    Leave my belongings around.
    Am not bothered by messy people.
    Am not bothered by disorder.

Dutifulness (.71)

+ keyed
    Try to follow the rules.
    Keep my promises.
    Pay my bills on time.
    Tell the truth.
    Listen to my conscience.

– keyed
    Break rules.
    Break my promises.
    Get others to do my duties.
    Do the opposite of what is asked.
    Misrepresent the facts.

Self-Discipline (.85)

+ keyed
    Get chores done right away.

Am always prepared.
Start tasks right away.
Get to work at once.
Carry out my plans.

– keyed

Find it difficult to get down to work.
Waste my time.
Need a push to get started.
Have difficulty starting tasks.
Postpone decisions.

Cautiousness (Deliberation) (.76)

+ keyed

Avoid mistakes.
Choose my words with care.
Stick to my chosen path.

– keyed

Jump into things without thinking.
Make rash decisions.
Like to act on a whim.
Rush into things.
Do crazy things.
Act without thinking.
Often make last-minute plans.

Altruism (.77)

+ keyed

Make people feel welcome.
Anticipate the needs of others.
Love to help others.
Am concerned about others.
Have a good word for everyone.

– keyed

Look down on others.
Am indifferent to the feelings of others.
Make people feel uncomfortable.
Turn my back on others.
Take no time for others.

Morality (Compliance) (.75)

+ keyed

Would never cheat on my taxes.
Stick to the rules.

– keyed
Use flattery to get ahead.
Use others for my own ends.
Know how to get around the rules.
Cheat to get ahead.
Put people under pressure.
Pretend to be concerned for others.
Take advantage of others.
Obstruct others' plans.

Imagination (Fantasy) (.83)

+ keyed
Have a vivid imagination.
Enjoy wild flights of fantasy.
Love to daydream.
Like to get lost in thought.
Indulge in my fantasies.
Spend time reflecting on things.

– keyed
Seldom daydream.
Do not have a good imagination.
Seldom get lost in thought.
Have difficulty imagining things.

Intellect (Ideas) (.86)

+ keyed
Like to solve complex problems.
Love to read challenging material.
Have a rich vocabulary.
Can handle a lot of information.
Enjoy thinking about things.

– keyed
Am not interested in abstract ideas.
Avoid philosophical discussions.
Have difficulty understanding abstract ideas.
Am not interested in theoretical discussions.
Avoid difficult reading material.

Positive Emotions (.81)

+ keyed
Radiate joy.
Have a lot of fun.
Express childlike joy.

Laugh my way through life.
Love life.
Look at the bright side of life.
Laugh aloud.
Amuse my friends.

– keyed

Am not easily amused.
Seldom joke around.

Appendix E: Big-Five Personality Factors (IPIP)

On the following page, there are phrases describing people's behaviors. Please use the rating scale below to describe how accurately each statement describes you. Describe yourself as you generally are now, not as you wish to be in the future. Describe yourself as you honestly see yourself, in relation to other people you know of the same sex as you are, and roughly your same age. So that you can describe yourself in an honest manner, your responses will be kept in absolute confidence.

Please read each statement carefully, and then select an option on the scale.
Response Options: 1 = "Very Inaccurate"; 2 = "Moderately Inaccurate"; 3 = "Neither Inaccurate nor Accurate"; 4 = "Moderately Accurate"; 5 = "Very Accurate"

Extraversion (.87)

+ keyed

Am the life of the party.
Feel comfortable around people.
Start conversations.
Talk to a lot of different people at parties.
Don't mind being the center of attention.

– keyed

Don't talk a lot.
Keep in the background.
Have little to say.
Don't like to draw attention to myself.
Am quiet around strangers.

Agreeableness (.82)

+ keyed

Am interested in people.
Sympathize with others' feelings.
Have a soft heart.
Take time out for others.
Feel others' emotions.
Make people feel at ease.

– keyed

Am not really interested in others.
Insult people.
Am not interested in other people's problems.
Feel little concern for others.

Conscientiousness (.79)

+ keyed

Am always prepared.
Pay attention to details.
Get chores done right away.
Like order.
Follow a schedule.
Am exacting in my work.

– keyed

Leave my belongings around.
Make a mess of things.
Often forget to put things back in their proper place.
Shirk my duties.

Emotional Stability (.86)

+ keyed

Am relaxed most of the time.
Seldom feel blue.

– keyed

Get stressed out easily.
Worry about things.
Am easily disturbed.
Get upset easily.
Change my mood a lot.
Have frequent mood swings.
Get irritated easily.
Often feel blue.

Intellect or Imagination (.84)

+ keyed

Have a rich vocabulary.
Have a vivid imagination.
Have excellent ideas.
Am quick to understand things.
Use difficult words.
Spend time reflecting on things.
Am full of ideas.

– keyed

Have difficulty understanding abstract ideas.
Am not interested in abstract ideas.
Do not have a good imagination.

Appendix F: Cybersecurity Climate Scale

Please answer on a scale of 1 (Strongly disagree) to 5 (Strongly agree) about how you feel the statement reflect your own views.

1. Issues related to the protection of private data are discussed in my workplace.
2. My supervisor frequently checks to see if we are all obeying rules related to the protection of private data.
3. Throughout the work week, my supervisor frequently talks about issues related to the protection of private data.
4. My supervisor says a good word whenever he sees actions taken that promote the protection of private data.
5. In my workplace it is worthwhile to put extra effort into protecting private data.
6. In my workplace it is important to maintain the protection of private data at all times.
7. In my workplace it is important to reduce the risk of data breaches.
8. In my workplace in order to get the work done, one must ignore some policies related to the protection of private data.
9. In my workplace, policies and procedures regarding the protection of private data are routinely ignored.
10. In my workplace, ignoring procedures regarding the protection of private data is acceptable.
11. My supervisor expects me to cut corners regarding the protection of private data and work faster when work is behind schedule.

Appendix G: Safety Climate Scale

Please answer on a scale of 1 (Strongly disagree) to 5 (Strongly agree) about how you feel the statement reflect your own views.

1. New employees learn quickly that they are expected to follow good health and safety practices.
2. Employees are told when they do not follow good health and safety practices.
3. Workers and management work together to ensure the safest possible conditions.
4. There are no major shortcuts taken when worker health and safety are at stake.
5. The health and safety of workers is a high priority with management where I work.
6. I feel free to report safety problems where I work.

Appendix H: Perceived Behavioral Control Scale

Please answer on a scale of 1 (Strongly disagree) to 5 (Strongly agree) about how you feel the statement reflect your own views.

1. Keeping my confidential information safe is beyond my control.
2. I believe that it is within my control to protect myself from information security violations.
3. The primary responsibility for protecting my confidential information belongs to myself.

Appendix I: Cybersecurity Behavior Scale

Please answer on a scale of 1 (Strongly disagree) to 5 (Strongly agree) about how you feel the statement reflect your own views.

1. I follow my organization's cybersecurity policies.
2. I comply with organizational IS security policies to protect the organization's information systems.
3. I follow organizational policies with regard to computer usage.

Appendix J: IRB Approval Letter

UNIVERSITY OF SOUTH FLORIDA

RESEARCH INTEGRITY AND COMPLIANCE
Institutional Review Boards, FWA No. 00001669
12901 Bruce B. Downs Blvd., MDC035 • Tampa, FL 33612-4799
(813) 974-5638 • FAX (813) 974-7091

October 23, 2017

David Howard
Psychology
St. Pete Beach, FL 33706

RE: **Exempt Certification**
IRB#: Pro00030997
Title: Development of the Cybersecurity Attitudes Scale and Modeling Cybersecurity Behaviors and its Antecedents

Dear Mr. Howard:

On 10/21/2017, the Institutional Review Board (IRB) determined that your research meets criteria for exemption from the federal regulations as outlined by 45CFR46.101(b):

(2) Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior, unless:
(i) information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and (ii) any disclosure of the human subjects' responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation.

As the principal investigator for this study, it is your responsibility to ensure that this research is conducted as outlined in your application and consistent with the ethical principles outlined in the Belmont Report and with USF HRPP policies and procedures.

Please note, as per USF HRPP Policy, once the Exempt determination is made, the application is closed in ARC. Any proposed or anticipated changes to the study design that was previously declared exempt from IRB review must be submitted to the IRB as a new study prior to initiation of the change. However, administrative changes, including changes in research personnel, do not warrant an amendment or new application.

Given the determination of exemption, this application is being closed in ARC. This does not limit your ability to conduct your research project.

We appreciate your dedication to the ethical conduct of human subject research at the University of South Florida and your continued commitment to human research protections. If you have any questions regarding this matter, please call 813-974-5638.

Sincerely,

Mark Ruiz, PhD, Vice
Chairperson USF Institutional
Review Board